

# **Tesis doctoral**

Adaptación de modelos de datos tácticos  
de sistemas de información para mando y  
control a la gestión de emergencias

Autor: Federico Carvajal Rodrigo  
Director: Manuel Esteve Domingo



*Ad memoriam matre mea*



## INDICE DE CONTENIDOS

<b>1</b>	<b>INTRODUCCIÓN Y OBJETIVOS .....</b>	<b>11</b>
1.1	Introducción .....	11
1.2	Objetivos de la Tesis.....	13
<b>2</b>	<b>ESTADO DEL ARTE DE LOS MODELOS DE DATOS TÁCTICOS .....</b>	<b>17</b>
2.1	Definición de Modelo de Datos.....	17
2.2	Metodología de modelado de datos.....	19
2.3	Historia y cronología de los modelos de datos tácticos.....	21
2.4	El Concepto de Generic Hub (GH).....	25
2.5	<b>El Land Command and Control Information Exchange Data Model (LC2IEDM) .....</b>	<b>32</b>
2.5.1	El LC2IEDM v2 .....	32
2.5.2	El LC2IEDM v5 .....	36
2.5.3	Resumen de la comparación de las versiones del LC2IEDM.....	39
2.6	<b>El Command and Control Information Exchange Data Model (C2IEDM).....</b>	<b>40</b>
2.6.1	C2IEDM Versión 6.1 .....	41
2.6.2	C2IEDM Versiones 6.15 (a, b, c, d, e) .....	46
2.6.2.1	Análisis de las diferentes versiones del modelo C2IEDM v6.15 .....	46
2.7	<b>Joint Consultation Command and Control Information Exchange Data Model (J3CIEDM) ..</b>	<b>51</b>
2.7.1	El J3CIEDM Ed 3.0.....	51
2.7.2	El J3CIEDM Ed 3.1.....	54
2.7.3	Resumen de la comparación de las versiones del J3CIEDM.....	59
<b>3</b>	<b>DISEÑO E IMPLEMENTACIÓN DE MODELOS DE DATOS Y MECANISMOS DE INTEROPERABILIDAD APLICABLES A LA GESTIÓN DE EMERGENCIAS CIVILES .....</b>	<b>63</b>
3.1	Introducción .....	63
3.2	Aplicación de los C2IS a la gestión conjunta de emergencias civiles .....	63
3.3	<b>Implementación del esquema físico del C2IEDM versión 6.15c.....</b>	<b>68</b>
3.3.1	Objetos de interés .....	70
3.3.2	Situación.....	75
3.3.3	Actividad .....	81
3.3.4	Agrupación de datos .....	84
3.4	<b>Implementación del esquema físico del J3CIEDM Ed 3.0.....</b>	<b>88</b>
3.5	<b>Interoperabilidad entre sistemas de mando y control.....</b>	<b>94</b>
3.5.1	Descripción e implementación de la solución MIP .....	94
3.5.1.1	La base de datos MIRD (Mip Information Resource Dictionary).....	95
3.5.1.2	Descripción del mecanismo de réplica de datos DEM.....	96
3.5.1.3	Implementación del mecanismo de réplica de datos DEM .....	98
3.5.1.4	Descripción e implementación del estándar NFFI .....	107
3.5.1.5	Implementación del uso del formato de mensajes NFFI.....	117

<b>4</b>	<b>VALIDACIÓN DE UN MODELO DE DATOS TÁCTICO PARA LA GESTIÓN DE EMERGENCIAS.....</b>	<b>125</b>
4.1	Introducción .....	125
4.2	Descripción del sistema SIMACOP .....	125
4.3	Diseño del núcleo común de un modelo de datos para emergencias civiles e implementación del mismo en el sistema SIMACOP .....	130
4.4	Validación del modelo.....	136
4.4.1	Demostración del sistema SIMACOP en el CWID nacional 2006.....	136
4.4.1.1	Descripción funcional de la demostración .....	137
4.4.1.2	Descripción técnica de la demostración.....	141
4.4.2	Evaluación de SIMACOP en su demostración en el CWID nacional 2006 (EP-31 CWID06) ....	148
4.4.3	Integración de SIMACOP con SIMACET .....	152
4.4.4	Pruebas de interoperabilidad NFFI del sistema SIMACOP en la demostración internacional CWID 2007 .....	156
4.4.4.1	Descripción los objetivos e hitos de la demostración internacional CWID 2007 .....	156
4.4.4.2	Requerimientos necesarios para la demostración CWID 2007 .....	157
4.4.4.3	Países y sistemas participantes en la demostración CWID 2007 .....	159
4.4.4.4	Fases de la demostración internacional CWID 2007 .....	160
4.4.4.5	Especificación del interfaz utilizado en los experimentos del CWID 07.....	160
4.4.4.6	Configuración del sistema de la demostración CWID 2007 .....	162
4.4.4.7	Evaluación de los resultados.....	164
4.4.4.8	Descripción de los experimentos .....	165
4.4.4.9	Descripción detallada de las pruebas realizadas al sistema SIMACOP .....	166
4.4.5	Evaluación de SIMACOP en su demostración en el CWID internacional 2007 .....	205
<b>5</b>	<b>CONCLUSIONES FINALES Y TRABAJO FUTURO.....</b>	<b>209</b>
5.1	Conclusiones finales .....	209
5.2	Trabajo futuro.....	214
<b>6</b>	<b>REFERENCIAS .....</b>	<b>217</b>

## INDICE DE FIGURAS

<b>Figura 1</b>	La metodología de modelado ER	20
<b>Figura 2</b>	El concepto de núcleo genérico y las distintas áreas funcionales.	26
<b>Figura 3</b>	Esquema genérico del uso del Mip Common Interface	27
<b>Figura 4</b>	Esquema de la topología centralizada	28
<b>Figura 5</b>	Esquema de la topología descentralizada	29
<b>Figura 6</b>	Esquema de la topología híbrida	30
<b>Figura 7</b>	Relaciones entre las cinco entidades clave del LC2IEDM v2	33
<b>Figura 8</b>	Visión general del modelo LC2IEDM v2	34
<b>Figura 9</b>	Relaciones entre las nueve entidades clave del LC2IEDM v5	37
<b>Figura 10</b>	Visión general del modelo LC2IEDM v5	38
<b>Figura 11</b>	Diagrama de las entidades independientes del C2IEDM v6.1	44
<b>Figura 12</b>	Visión general del modelo C2IEDM v6.1	45
<b>Figura 13</b>	Estructura de la entidad ACTION-LOCATION del modelo C2IEDM v6.15b	47
<b>Figura 14</b>	Definición de las fronteras entre unidades del modelo C2IEDM v6.15b	48
<b>Figura 15</b>	Definición de las fronteras entre unidades del modelo C2IEDM v6.15c	49
<b>Figura 16</b>	Entidades independientes del modelo J3CIEDM Edition.3.1	57
<b>Figura 17</b>	Escenario inicial del ejemplo de la crisis civil	64
<b>Figura 18</b>	Escenario final del ejemplo de la crisis civil	66
<b>Figura 19</b>	Tablas de la base de datos del esquema físico del C2IEDM v6.15c	68
<b>Figura 20</b>	Relaciones de la base de datos del esquema físico del C2IEDM v6.15c	69
<b>Figura 21</b>	Primeros niveles de la jerarquía de los objetos ítem y tipo	71
<b>Figura 22</b>	Estructura jerárquica completa de la entidad OBJECT-ITEM	73
<b>Figura 23</b>	Estructura jerárquica completa de la entidad OBJECT-TYPE	74
<b>Figura 24</b>	Estructura jerárquica completa de la entidad OBJECT-ITEM-STATUS	75
<b>Figura 25</b>	Estructura jerárquica completa de la entidad ADDRESS	76
<b>Figura 26</b>	Estructura jerárquica completa de la entidad LOCATION	78
<b>Figura 27</b>	Estructura jerárquica completa de la entidad CAPABILITY	80
<b>Figura 28</b>	Estructura jerárquica completa de la entidad ACTION	82
<b>Figura 29</b>	Estructura jerárquica completa de la entidad REPORTING-DATA	85
<b>Figura 30</b>	Estructura jerárquica completa de la entidad CONTEXT	86
<b>Figura 31</b>	Tablas de la base de datos del esquema físico del JC3IEDM Edition.3.0	88

<b>Figura 32</b>	Relaciones de la base de datos del esquema físico del JC3IEDM Edition.3.0	89
<b>Figura 33</b>	Estructura jerárquica completa de la entidad OBJECT-TYPE	91
<b>Figura 34</b>	Estructura jerárquica completa de la entidad ACTION	92
<b>Figura 35</b>	Estructura jerárquica completa de la entidad OBJECT-ITEM	93
<b>Figura 36</b>	Descripción de la arquitectura del Data Exchange Mechanism (DEM)	97
<b>Figura 37</b>	Tablas del esquema físico de la BD MIRD del C2IEDM v6.15c	99
<b>Figura 38</b>	Relaciones del esquema físico de la BD MIRD del C2IEDM v6.15c	99
<b>Figura 39</b>	Diagrama de estados generado para el (DP)	100
<b>Figura 40</b>	Diagrama de estados generado para el (DR)	101
<b>Figura 41</b>	Descripción del proceso completo de réplica implementado	105
<b>Figura 42</b>	Esquema de la sección <i>positionalData</i> del mensaje NFFI 1.3	110
<b>Figura 43</b>	Esquema de la sección <i>identificationData</i> del mensaje NFFI 1.3	111
<b>Figura 44</b>	Esquema de la sección <i>operStatusData</i> del mensaje NFFI 1.3	111
<b>Figura 45</b>	Esquema de la sección <i>deviceSpecificData</i> del mensaje NFFI 1.3	112
<b>Figura 46</b>	Esquema de la sección <i>detailData</i> del mensaje NFFI 1.3	112
<b>Figura 47</b>	Esquema de la estructura completa del mensaje NFFI 1.3	113
<b>Figura 48</b>	Esquema de funcionamiento del estándar NFFI v1.3	118
<b>Figura 49</b>	Esquema físico de la base de datos intermedia para mensajes NFFI	120
<b>Figura 50</b>	Proceso de réplica de posiciones utilizando el estándar NFFI	121
<b>Figura 51</b>	Estructura de planos propuesta por el DoD	127
<b>Figura 52</b>	Arquitectura de red del sistema SIMACOP	129
<b>Figura 53</b>	Vista del núcleo común del modelo de datos de SIMACOP	132
<b>Figura 54</b>	Descripción funcional del núcleo común del sistema SIMACOP	133
<b>Figura 55</b>	Pantalla del nodo SIMACOP de C2 a nivel de secciones	139
<b>Figura 56</b>	Pantalla del nodo SIMACOP de C2 a nivel de sección/pelotones	139
<b>Figura 57</b>	Pantalla del nodo SIMACOP de C2 a nivel de pelotón/unidades	140
<b>Figura 58</b>	Pantalla del nodo SIMACOP de C2 a nivel de unidades de tropa	140
<b>Figura 59</b>	Esquema técnico de la demostración a nivel de nodo C2	141
<b>Figura 60</b>	Esquema completo del despliegue realizado	142
<b>Figura 61</b>	Equipamiento de la patrulla real que participó la demostración	143
<b>Figura 62</b>	Detalle de los sensores biométricos	143
<b>Figura 63</b>	Detalle del Tablet PC utilizado en la demostración	143
<b>Figura 64</b>	Vehículo del tipo Rioja empleado durante la demostración	144



<b>Figura 65</b> Nodo de nivel de Secciones y nodo de nivel de Sección/Pelotones	145
<b>Figura 66</b> Detalle de la réplica de datos en los nodos C2 de SIMACOP	146
<b>Figura 67</b> Flujos de información SIMACET-SIMACOP-NFFI	153
<b>Figura 68</b> Configuración global de la demostración CWID 2007	162

## INDICE DE TABLAS

<b>Tabla 1.</b> Definición de las cinco entidades clave del LC2IEDM v2 y sus roles.	33
<b>Tabla 2.</b> Definición de las nueve entidades clave del LC2IEDM v5 y sus roles.	37
<b>Tabla 3.</b> Definición de las entidades independientes del C2IEDM v6.1 y sus roles.	43
<b>Tabla 4</b> Entidades renombradas en el J3CIEDM por cambios estructurales	52
<b>Tabla 5</b> Entidades renombradas en el J3CIEDM por requerimientos CBRN	53
<b>Tabla 6</b> Cambios en las palabras clase de los atributos en el J3CIEDM Ed.3.0	53
<b>Tabla 7.</b> Definición de las entidades independientes del J3CIEDM Ed 3.1 y sus roles	56
<b>Tabla 8.</b> Entidades subtipo de primer nivel tanto de objetos ítem como de objetos tipo	72
<b>Tabla 9.</b> Tablas y atributos del núcleo común del modelo de datos de SIMACOP	131
<b>Tabla 10</b> Países y sistemas participantes en la demostración CWID 2007	159
<b>Tabla 11</b> Lista de medidas de desarrollo o Measures of Performance (MoP)	164
<b>Tabla 12</b> Listado de experimentos de la demostración CWID 2007	165
<b>Tabla 13</b> Descripción del experimento 403	167
<b>Tabla 14</b> Descripción del experimento 405	169
<b>Tabla 15</b> Descripción del experimento 409	171
<b>Tabla 16</b> Descripción del experimento 411	173
<b>Tabla 17</b> Descripción del experimento 460	174
<b>Tabla 18</b> Descripción del experimento 480	176
<b>Tabla 19</b> Descripción del experimento 482	178
<b>Tabla 20</b> Descripción del experimento 484	180
<b>Tabla 21</b> Descripción del experimento 485	182
<b>Tabla 22</b> Descripción del experimento 531	184
<b>Tabla 23</b> Descripción del experimento 532	186
<b>Tabla 24</b> Descripción del experimento 639	188
<b>Tabla 25</b> Descripción del experimento 640	190
<b>Tabla 26</b> Descripción del experimento 1512	192
<b>Tabla 27</b> Descripción del experimento 1513	194
<b>Tabla 28</b> Descripción del experimento 1542	196
<b>Tabla 29</b> Descripción del experimento 1549	198
<b>Tabla 30</b> Descripción del experimento 1558	200
<b>Tabla 31</b> Descripción del experimento 1568	202

<b>Tabla 32</b> Descripción del experimento 1587	204
<b>Tabla 33</b> Resumen de la evaluación de las pruebas en las que ha participado SIMACOP	205



---

## SECCIÓN 1



# 1 Introducción y Objetivos

## 1.1 Introducción

*“No basta con adquirir sabiduría, es preciso además saber usarla.”*

Marco Tulio Cicerón

La información a la hora de gestionar la resolución de una crisis es vital y mucho más en nuestros días, donde se dispone de muchos y muy heterogéneos sistemas, para difundirla por distintos canales (radio, telefonía, televisión, redes privadas, Internet, etc.) y en distintos formatos (audio, video, imágenes, datos, etc.)

Esta afirmación se puede aplicar perfectamente a la gestión de crisis en ámbito civil, ya que cuanto más información se posea sobre una crisis y mejor se pueda coordinar a los efectivos encargados de mitigar dicha crisis, esta se resolverá de una forma más óptima.

Esta gran variedad de formatos y medios para difundir la información, que en un principio se puede considerar una gran ventaja, puede llegar a convertirse en algunas ocasiones en un grave problema a la hora de coordinar recursos pertenecientes a distintas entidades, como podrían ser por ejemplo, unidades militares pertenecientes a distintos países durante una operación conjunta, o los diferentes servicios de emergencias y cuerpos de seguridad encargados de mitigar una grave crisis en el entorno civil; bomberos, policía, servicios sanitarios e incluso unidades militares en misión de apoyo.

Por otro lado, todas las operaciones militares amparadas por las Naciones Unidas actualmente se llevan a cabo actualmente de forma conjunta por países aliados, durante el transcurso de estas operaciones conjuntas vemos que cada país e incluso en ocasiones, cada arma dentro del ejército de un mismo país, cuenta con su propio sistema de mando y control e información, o Command and Control Information Systems C2IS utilizando la terminología anglosajona, para coordinar sus efectivos.

Esta variedad en lo que se refiere a sistemas C2I, puede plantear graves problemas de interoperabilidad a la hora de coordinar unidades de diferentes países en estas operaciones conjuntas, problemas planteados principalmente, a la hora de compartir información entre los distintos C2IS con el fin de poder tener una visión común de la situación o Common Operational Picture, (COP).

Los principales problemas de interoperabilidad entre los distintos C2IS de los diferentes países, se deben principalmente a las diferencias a la hora de definir o modelar los datos [1] [2], que se tienen que compartir durante las operaciones conjuntas, con el objetivo de obtener la COP y tener un conocimiento general de la situación o Situation Awareness, (SA).

Por lo que se refiere al modelado de estos datos, vemos que cada entidad susceptible de ser utilizada o participar en una operación militar es modelada, para poder ser tratada y almacenada como un dato por un C2IS. El modelado de todos estos datos y el conjunto de todas sus relaciones, forman el modelo de datos de cada C2IS.

Estos modelos de datos suelen responder a las necesidades tácticas y operativas específicas que cada país considera oportunas para su C2IS, por lo tanto, cada modelo de datos de cada C2IS será único y para complicar aun más la situación, en muchas ocasiones la información que se modela es de naturaleza reservada.

Un ejemplo muy gráfico sería la definición o el modelado de una persona, en un determinado modelo de datos A, la entidad persona puede tener como atributos un identificador de 9 dígitos, su edad en años, su estatura en metros, su nacionalidad y su rango militar. En otro modelo de datos B, los atributos de la misma persona podrían ser un identificador de 15 dígitos, su género, edad en años, estatura en pies y pulgadas y su religión.

Todo ello dependiendo en cada caso de los atributos que cada país haya considerado más oportunos para modelar una persona dentro de su C2IS. Al intentar intercambiar información sobre personas, los sistemas C2I A y C2I B no podrán hacerlo, aun cuando se trate de la misma persona que haya sido modelada en ambos sistemas, pero con atributos claramente diferentes en cada uno de ellos, e incluso con unidades distintas en algunos atributos coincidentes.

Con esta situación, el hecho de compartir información en tiempo pseudo real y obtener una COP durante una operación militar conjunta, resulta una tarea ingente y en muchas ocasiones imposible, aun cuando se cuenten con los sistemas y equipos más sofisticados en materia de electrónica y telecomunicaciones.

Todos estos problemas a una menor escala y algunos nuevos derivados del entorno civil, se pueden dar durante la gestión de las crisis civiles [3] en las que intervienen y han de coordinarse entre sí mediante sus distintas escalas de mando, unidades de los servicios de emergencias y de los distintos cuerpos y fuerzas de seguridad del estado, así como en algunos casos graves, unidades militares en labores de apoyo como se ha dicho anteriormente.

De cara a obtener interoperabilidad entre agencias (bomberos, policía, servicios sanitarios e incluso unidades militares en misión de apoyo), y entre distintos países, en caso de operaciones internacionales, parece razonable definir un modelo de datos común para la gestión de emergencias civiles derivado de los modelos de datos militares como por ejemplo el Command and Control Information Exchange Data Model (C2IEDM).

La reciente creación de la unidad militar de emergencias (UME), supone una confirmación del planteamiento de la presente tesis y de la línea de investigación del grupo de Sistemas de Tiempo Real Distribuidos de la UPV.



## 1.2 Objetivos de la Tesis

Con la presente Tesis doctoral se pretende profundizar en la problemática del modelado de datos en el ámbito militar, analizar las diferentes soluciones de interoperabilidad entre sistemas C2IS que se han propuesto y las que se están experimentando en la actualidad, para adaptarlas al entorno de la gestión y coordinación de crisis civiles en las que participan distintos cuerpos de seguridad y servicios de emergencia.

Para conseguir este objetivo global se deberán alcanzar los siguientes objetivos parciales;

- Realizar un exhaustivo análisis del estado del arte del modelado de datos para sistemas C2I militares, desde sus comienzos hasta los últimos experimentos de interoperabilidad de la Organización del Tratado del Atlántico Norte (OTAN). Será analizada con especial interés la iniciativa internacional Multilateral Interoperability Program MIP [4], que es la entidad encargada del desarrollo y actualización del sistema de interoperabilidad adoptado por la OTAN.

Este análisis nos permitirá tener una idea clara de la evolución del modelado de datos en el ámbito militar y poder seguir las tendencias e iniciativas internacionales encaminadas a resolver los problemas de interoperabilidad planteados, en las operaciones conjuntas, debido a la falta de correlación de los distintos modelos de datos de los sistemas C2I de los países aliados.

- Una vez analizada en profundidad la problemática del modelado de datos para sistemas C2I militares y sus posibles soluciones, se estudiarán los modos de coordinación y gestión de crisis civiles de gran magnitud, atendiendo principalmente a la resolución de los problemas de mando, control y coordinación de recursos detectados, en algunas de las mayores crisis que se han desencadenado en los últimos tiempos; 11S en Nueva York o el tsunami del 2004 en Indonesia.
- Implementar y comparar las soluciones de interoperabilidad más extendidas actualmente, describiendo los procesos operativos de intercambio de datos. Con los resultados obtenidos se propondrá un modelo de datos para ser usado en la gestión de emergencias el ámbito civil.
- El modelo de datos propuesto, se incluirá dentro de una solución de sistema de detección y seguimiento de recursos, que podrá ser usado por los distintas agencias que participasen en la gestión de crisis civiles de todo tipo, desde grandes inundaciones a ataques terroristas a gran escala.
- Con las conclusiones a las que se llegue después del trabajo realizado se intentará poner de manifiesto las actuales carencias en la gestión de crisis civiles en lo que se refiere a la coordinación de diferentes estamentos o servicios de emergencias, y como esta coordinación podría mejorarse con la inclusión de sistemas de detección y seguimiento de recursos dotados de comunicaciones en tiempo real e interoperables entre sí.

De esta forma se tendría una COP en todos los estamentos al mando de las distintas agencias implicadas en la mitigación de la crisis, pudiéndose tomar decisiones mucho más ajustadas a la situación real y optimizar el tiempo de respuesta y la eficacia de los recursos.



---

## SECCIÓN 2



## 2 Estado del arte de los Modelos de Datos tácticos

### 2.1 Definición de Modelo de Datos

Existen en la literatura científica numerosas definiciones de modelo de datos, después de consultar muchas de ellas, las que mejor definen el concepto de modelo de datos aplicable a la temática de la presente tesis doctoral serían las siguientes;

Según la primera definición se denomina modelo:

“...al instrumento que se aplica a una parcela del mundo real (universo del discurso) para obtener una estructura de datos a la que denominamos esquema. Esta distinción entre el modelo (instrumento) y el esquema (resultado de aplicar el instrumento) es importante. Es importante también distinguir entre mundo real y universo del discurso, ya que este último es la visión que del mundo real tiene el diseñador...”

Podemos definir pues un *modelo de datos*, como un conjunto de conceptos, reglas y convenciones que nos permiten describir los datos del universo del discurso.” [5]

La segunda definición nos dice que “el *modelo de datos*, como abstracción del universo de discurso, es el enfoque utilizado para la representación de entidades y sus características (relaciones, atributos) dentro de una base de datos” [6].

Una vez se ha definido formalmente el concepto de modelo de datos, se van a enumerar los tres principales tipos de modelos de datos existentes:

1. **Modelos lógicos basados en objetos:** los dos más extendidos son el modelo entidad-relación y el orientado a objetos.

- El modelo entidad-relación (ER) se basa en una percepción del mundo compuesta por objetos, llamados entidades, y relaciones entre ellos. Las entidades se diferencian unas de otras a través de atributos.
- El modelo entidad-relación extendido (EER), que es el mismo modelo entidad relación anterior al que se le han añadido otros conceptos, como los atributos compuestos y las jerarquías de generalización.
- El orientado a objetos también se basa en objetos, los cuales contienen valores y métodos, entendidos como órdenes que actúan sobre los valores, en niveles de anidamiento. Los objetos se agrupan en clases, relacionándose mediante el envío de mensajes. Algunos autores definen estos modelos como "modelos semánticos".

2. **Modelos lógicos basados en registros:** el más extendido es el relacional, mientras que los otros dos existentes, jerárquico y de red, se encuentran en retroceso. Estos modelos se usan para especificar la estructura lógica global de la base de datos, estructurada en registros de formato fijo de varios tipos.

- El modelo relacional representa los datos y sus relaciones mediante tablas bidimensionales, que contienen datos tomados de los dominios correspondientes.
- El modelo de red está formado por colecciones de registros, relacionados mediante punteros o ligas en grafos arbitrarios.

- El modelo jerárquico es similar al de red, pero los registros se organizan como colecciones de árboles. Algunos autores definen estos modelos como "modelos de datos clásicos".

3. **Modelos físicos de datos:** muy poco usados, son el modelo unificador y el de memoria de elementos. Algunos autores definen estos modelos como "modelos de datos primitivos".

## **2.2 Metodología de modelado de datos**

Para trasladar el mundo real o el universo del discurso a una estructura de datos, se debe emplear una metodología de modelado, que permita obtener una estructura de datos almacenada en una base de datos a partir de los objetos del mundo real y que pueda ser accedida por una aplicación de gestión de bases de datos.

Existen dos metodologías principales para la creación de modelos de datos: la metodología Entidad-Relación (ER) y la metodología de Modelo Objeto.

A continuación vamos a describir con detalle la aproximación ER [7], ya que es la utilizada para la creación de los modelos de datos tácticos que se analizarán en la presente tesis doctoral

La metodología de modelado ER nos permite transformar los objetos de la realidad en datos lógicos dentro una base de datos física. Esta metodología consiste principalmente en el desarrollo de tres tipos de modelos de datos, el conceptual, el lógico y el físico [8] [9], que a través de tres niveles de abstracción, permitirán obtener al final del proceso una estructura de datos lógicos dentro de una base de datos a partir de los objetos del mundo real.

**El modelo de datos conceptual o primer nivel de abstracción:** Este modelo se utiliza para representar la realidad con un alto nivel de abstracción. El objetivo del modelo conceptual es clarificar y simplificar la realidad. Los detalles no críticos del mundo real pueden dejarse a un lado en el modelado conceptual, para poder destacar con más fuerza las principales entidades, atributos y sus relaciones.

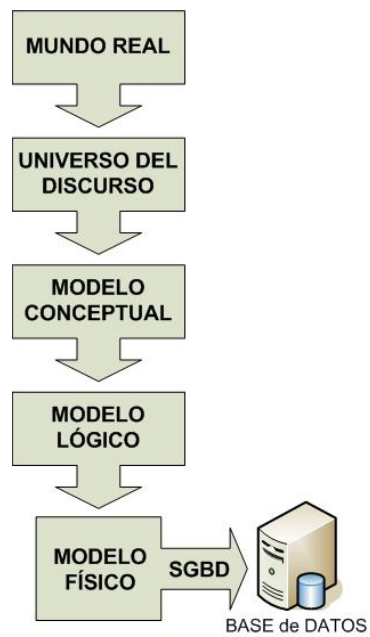
No es necesario descubrir ni documentar a este nivel, todos los atributos de cada entidad, además asuntos como la cardinalidad y los tipos de datos pueden ser obviados a nivel conceptual y solo algunas claves de algunas entidades son identificadas, debido al alto nivel de abstracción de este modelo.

**El modelo de datos lógico o segundo nivel de abstracción:** Este modelo debe ser un completo documento que describe una estructura de datos a través de la cual una base de datos puede ser generada. Consiste en un conjunto completo y normalizado de entidades con todos sus atributos, tipos de datos y cardinalidad de sus relaciones perfectamente definidos.

El modelo lógico requiere además, que las claves principales de las entidades que vayan a ser candidatas a convertirse en identificadores únicos de dichas entidades, queden perfectamente identificadas. Las claves foráneas y si las relaciones entre las distintas entidades son obligatorias u opcionales, también debe quedar claramente definido a este nivel.

**El modelo de datos físico o tercer nivel de abstracción:** Este modelo se crea para especificar de forma exacta como transformar el modelo de datos lógico en una base de datos física mediante un sistema gestor de bases de datos como puede ser DB2, Oracle o MySQL.

La metodología que se acaba de enunciar queda perfectamente descrita en el diagrama representado en la Figura 1



**Figura 1**

Una vez definidos y clarificados algunos conceptos básicos del modelado de datos y su metodología de abstracción, pasaremos a ver con detalle la evolución de los modelos de datos tácticos, que serán el núcleo de la investigación llevada a cabo en esta tesis doctoral.



### **2.3 Historia y cronología de los modelos de datos tácticos.**

Como ya se ha dicho en anteriores capítulos de esta tesis doctoral, el hecho de que las operaciones militares en las que participaba la OTAN requirieran cada vez más la cooperación de contingentes militares de diferentes naciones, hizo necesario iniciar nuevas investigaciones para ofrecer a los comandantes de dichas fuerzas una visión común del espacio de operaciones, esta visión común (COP) del espacio de operaciones se conseguiría mediante el intercambio preciso de información entre los sistemas de mando y control (C2) de las diferentes naciones participantes en cada operación.

Debido a esta circunstancia, el Comité Militar (MC) de la Organización de Tratado del Atlántico Norte (OTAN), aprobó la declaración MC 245 [10], el 18 de Junio de 1976 y el Consejo del Tratado del Atlántico norte la ratificó el 6 de agosto de 1976 (PO/76/87).

La declaración MC 245 fue una exposición de los requerimientos militares de interoperabilidad entre dos sistemas de datos automatizados. Esta declaración, cuyos principios siguen todavía hoy vigentes, permitió el comienzo de una iniciativa de investigación con el fin de valorar la viabilidad del desarrollo de un sistema militar táctico de mando, control e información común o Army Tactical Command and Control Information System (ATCCIS) [11], para ser implantado en la región central de control de la OTAN a largo plazo (siguientes 15 años).

Esta iniciativa de investigación se basó en los requerimientos especificados en programa de defensa a largo plazo o Long Term Defence Programme (LTDP) Task Force 6, que se formó en 1979 para desarrollar programas de mando, control y consulta o Consultation Command and Control (C3), a largo plazo tras la declaración MC 245. Nació así el programa ATCCIS en 1980.

El programa ATCCIS no fue un programa formal de la OTAN, ATCCIS comenzó como una actividad independiente y voluntaria de la que forman parte los siguientes países y cuarteles generales: Bélgica, Canadá, Republica Checa, Dinamarca, Francia, Alemania, Hungría, Italia, Holanda, Noruega, Polonia, Portugal, España, Turquía, Reino Unido, Estados Unidos, Cuarteles generales de las fuerzas aliadas de Europa del norte o Regional Headquarters Allied Forces North Europe (RHQ AFNORTH) y Los cuarteles generales supremos de las fuerzas aliadas en Europa o Supreme Headquarters Allied Powers Europe (SHAPE).

ATCCIS fue un programa que se dividió en 5 fases, la primera fue un estudio de viabilidad de un mecanismo para garantizar la interoperabilidad entre distintos sistemas de mando y control y estuvo activa entre 1980 y 1983, la segunda identificó los conceptos militares y técnicos requeridos para llevar a cabo interoperabilidad de sistemas de mando y control a través de intercambio automático de datos, esta fase estuvo activa entre 1985 y 1990, en la tercera fase se demostró con éxito la interoperabilidad de sistemas de mando y control que aplicaban el mecanismo definido por ATCCIS durante una demostración multinacional, esta fase estuvo activa entre 1992 y 1997, la cuarta fase se centro en refinar las especificaciones y en potenciar la transición de los sistemas de los países que componían ATCCIS, esta fase estuvo activa entre 1997 y 2000, en la quinta y última fase se completó la especificación dejándola lista para su incorporación a sistemas de mando y control reales, esta fase estuvo activa entre 2000 y 2002 y fue conocida como ATCCIS 2000.

Las especificaciones del mecanismo para garantizar la interoperabilidad entre sistemas de mando y control propuesto por el programa ATCCIS consistían principalmente en dos componentes: Un modelo de datos y un mecanismo de réplica.

El primer modelo de datos desarrollado por ATCCIS fue el “ATCCIS Battlefield Generic Hub Data Model”, conocido comúnmente como Generic Hub (GH), este primer modelo fue lanzado el 23 abril de 1993.

La investigación continuó y como consecuencia varias versiones de este modelo fueron lanzadas en los años siguientes:

- El ATCCIS Battlefield Generic Hub Level 2 Data Model: (Specification for the Demonstration) el 26 de agosto de 1994,
- El ATCCIS Battlefield Generic Hub 3 Data Model Specification Ed.1, el 12 de diciembre de 1996,
- El ATCCIS Battlefield Generic Hub 3 Data Model Specification Ed.2, el 19 de septiembre de 1997
- El ATCCIS Battlefield Generic Hub 3 Data Model Specification Ed.3, el 10 julio de 1998.

El 1 octubre de 1999 un borrador con una nueva versión del modelo de datos fue lanzado, pero en esta versión el modelo cambió su nombre a Land C2 Information Exchange (LC2IEDM) [12]. La primera versión estable del nuevo modelo fue la LC2IEDM v2 [13], que fue lanzada el 31 de marzo del 2000 junto con el ATCCIS Replication Mechanism ARM [14]. El LC2EDM v2 fue el núcleo del modelo de referencia OTAN y fue también la vista del modelo de datos conjunto de la OTAN (STANAG 5523 / AdatP-32) [15].

El ATCCIS Replication Mechanism (ARM), es complementario al modelo de datos LC2IEDM. Su principal objetivo es conseguir que cuando una aplicación de mando y control cambia el estado de parte de la información que guarda, y esta información cumple la especificación de ATCCIS, esta información sea automáticamente replicada a todos los demás sistemas de mando y control de la red que han acordado intercambiar esa información en concreto. Además el significado y la integridad de los datos replicados deben mantenerse sin ningún tipo de proceso en el receptor. Los gestores del sistema pueden decidir que información es la que fluye, cuando fluye y sobre que medio físico de comunicaciones.

El 18 de marzo de 2002 el programa ATCCIS en su fase final lanzó el modelo de datos LC2IEDM v.5 [16] y el modelo de replica ARM v5.

En paralelo al programa ATCCIS, los responsables del área conjunta de proyectos de sistemas de mando y control e información de los ejércitos de Canadá, Francia, Alemania, Italia, el Reino Unido y los Estados Unidos establecieron en abril de 1998 el programa multilateral de interoperabilidad o Multilateral Interoperability Programme (MIP), en Calgary, Canadá.

El programa MIP sustituía y potenciaba dos programas previos, el programa de interoperabilidad en el campo de batalla o Battlefield Interoperability Programme (BIP) y el programa de interoperabilidad cuadrilateral o Quadrilateral Interoperability Programme (QIP).

El objetivo principal del programa MIP es el completo desarrollo de los dos mecanismos siguientes:

- El mecanismo de intercambio de mensajes o Message Exchange Mechanism (MEM) [17], que mejoró las capacidades de los mensajes estructurados (ADatP-3) [18], facilitando la interoperabilidad tanto vertical como horizontal de los sistemas de mando y control e información a todos los niveles, desde cuerpo de ejército hasta batallón.
- El mecanismo de intercambio de datos o Data Exchange Mechanism (DEM) [19], que implementa el mecanismo de envío de datos que apoya la interoperabilidad tanto vertical como horizontal de los sistemas de mando y control e información a todos los niveles, desde cuerpo de ejército hasta batallón.

Los dos mecanismos desarrollados por MIP, tanto el DEM como el MEM, están basados en el Land C2 Information Exchange Data Model (LC2IEDM) de ATCCIS.

A finales del 2002 las actividades de ATCCIS y MIP eran muy semejantes, se compartieron informaciones y la tecnología y las especificaciones que ambos programas manejaban fueron casi comunes, la fusión de ambos programas fue considerado un paso natural y positivo y fue reconocido casi inmediatamente por la publicación de una directiva de respaldo al programa MIP por la OTAN [20].

El carácter y los objetivos de ATCCIS pasaron al programa MIP, que se vio fortalecido por la fusión con ATCCIS. Las naciones y los cuarteles generales que pasaron a formar parte del nuevo programa MIP fueron los siguientes: Australia, Austria, Bélgica, Canadá, República Checa, Dinamarca, Finlandia, Francia, Alemania, Grecia, Hungría, Italia, Lituania, Holanda, Noruega, Polonia, Portugal, Rumania, Eslovenia, España, Suecia, Turquía, Reino Unido, Estados Unidos, JFC Brunssum y el Allied Command Transformation (ACT).

El desarrollo continuó dentro del programa MIP con la inclusión de un mayor contenido orientado a operaciones conjuntas y el 20 de noviembre de 2003, una nueva versión del modelo de datos fue lanzada. A partir de aquí los conceptos no solo se suscribieron al ámbito de las operaciones terrestres y el nuevo modelo de datos se llamó Command and Control Information Exchange Data Model (C2IEDM) Edition 6.1 [21], requerimientos operacionales prioritarios hicieron que la versión 6.1 del C2IEDM tuviera que ser modificada, de esta forma el modelo de datos evolucionó y la versión 6.1.5a del C2IEDM [22] fue lanzada el 26 de septiembre de 2004.

Durante 2005 se publicaron 4 nuevas versiones del C2IEDM 6.1.5, a continuación se enumeran estas 4 nuevas versiones y su fecha de publicación;

- El C2IEDM Edition6.15b, se publicó el 17 de marzo de 2005. [23]
- El C2IEDM Edition6.15c, se publicó el 12 de julio de 2005. [24]
- El C2IEDM Edition6.15d, se publicó el 30 de septiembre de 2005. [25]
- El C2IEDM Edition6.15e, se publicó el 2 de diciembre de 2005. [26]

El programa MIP cuenta con un fuerte apoyo de la OTAN, este apoyo se vio reflejado en la firma del memorando de acuerdo o Memorandum of Agreement (MOA) entre MIP y el grupo de administración de datos de la OTAN o NATO Data Administration Group (NDAG) [27]

Las fases del programa MIP son las siguientes:

- Bloque 1 finalizada en noviembre del 2003 con la publicación del C2IEDM versión 6.
- Bloque 2 finalizada en 2005. Durante esta fase se implementó la versión 6 del C2IEDM y a finales del 2004 se produjo la fusión de dos modelos de datos para dar lugar al C2IEDM versión 7, más conocido como JC3IEDM Ed 0.5.

Los Detalles de esta fusión son los siguientes: El GH fue la base de la primera versión del modelo de referencia de la OTAN, que fue desarrollado hasta su versión 4, como respuesta al MOA entre MIP y la OTAN, la versión 4 del GH se fusionó con el C2IEDM v6.1 para dar como resultado, el 10 de diciembre de 2004, el Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM) Ed 0.5 [28].

La siguiente versión de este modelo fue el (JC3IEDM) Ed 3.0 [29], que se publicó el 9 de diciembre de 2005. Esta nueva edición del modelo de datos constituirá el contenido técnico del STANAG 5525 [30] de la OTAN.

El J3CIEDM continúa su evolución, incluyendo nuevos requerimientos y/o modificaciones, al igual que todos los anteriores modelos nombrados en este apartado. Así el 8 de diciembre de 2006 se publicó el Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM) Ed 3.1 [31]. Esta es la última edición del modelo publicada hasta el momento de escribir la presente tesis doctoral.

## **2.4 El Concepto de Generic Hub (GH)**

Uno de los principales resultados del programa ATCCIS fue la creación del Generic Hub Data Model, más conocido como Generis Hub (GH). Este modelo de datos fue diseñado para convertirse en una solución universal que facilitara la interoperabilidad de los futuros sistemas de mando, control e información de las naciones que formaban parte del programa. El mismo concepto continuó vigente en las siguientes versiones del GH, tras la fusión entre los programas ATCCIS y MIP.

Este concepto de modelo de datos genérico permitía a todas las naciones construir sus sistemas de mando y control con su propia “visión del mundo”, es decir, elaborando las abstracciones de sus modelos de datos como considerasen más conveniente, pero manteniendo un núcleo común (GH) de datos estándar, que facilitaría el entendimiento y el intercambio de datos entre los distintos sistemas de mando y control, de esta forma se conseguía que varios sistemas de mando y control con arquitecturas heterogéneas pudieran interoperar entre sí.

La viabilidad técnica del sistema fue demostrada durante el programa Joint Warrior Interoperability Demonstrator (JWID), finalmente el modelo de datos desarrollado por ATCCIS llegó a convertirse en un estándar OTAN con la publicación número 32 del mando aliado ADatP-32 con el nombre de Land Command and Control Information Exchange Data Model (LC2IEDM) en 1999.

Como ya se ha dicho, el modelo de datos genérico (GH), primero con ATCCIS y luego con MIP, evolucionó en sus diferentes versiones, pero el concepto inicial permaneció intacto:

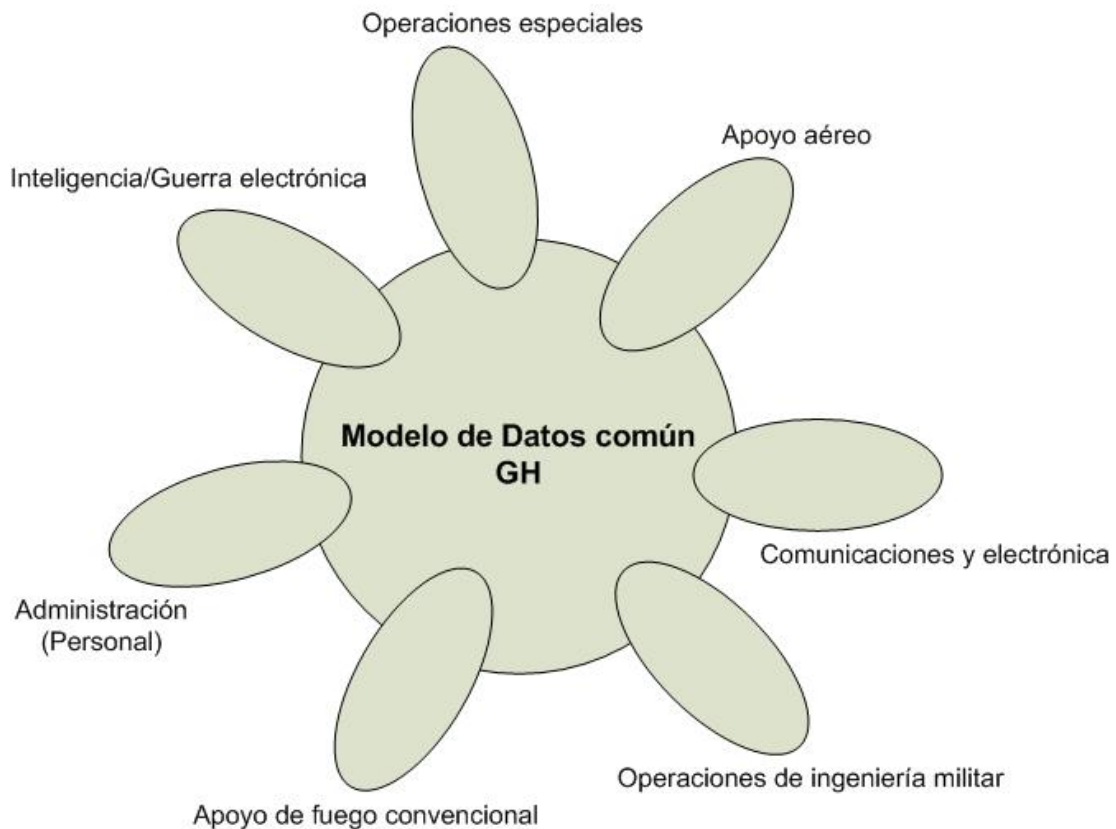
Un núcleo común de datos, estructurados de una manera estándar que permitan por un lado, aglutinar la información común de múltiples áreas funcionales o Sub-Functional Areas (SFA) del propio sistema de mando y control, convirtiéndose así en el concentrador o Hub, que unifica la estructura de los datos común a las distintas SFA y por el otro lado, permitir intercambiar toda la información necesaria entre dos sistemas de mando y control distintos para conseguir su interoperabilidad.

La aplicación de este concepto aseguraría que todos los datos que son susceptibles de ser intercambiados entre las distintas áreas funcionales, (apoyo de fuego convencional, operaciones de ingeniería militar, comunicaciones y electrónica, operaciones especiales, apoyo aéreo, etc.), estuvieran estructurados de una forma estándar en el núcleo común o concentrador (GH).

En resumen, el Generis Hub Data Model en cualquiera de sus versiones (LC2IEDM, C2IEDM v6.1, C2IEDM v6.15a, C2IEDM v6.15b, etc.) intenta representar el núcleo de los datos identificados como susceptibles de ser intercambiados entre las distintas áreas funcionales y entre otros sistemas de mando y control distintos.

De esta forma, el GH describe de una forma estandarizada todos los objetos de interés del espacio de operaciones, como por ejemplo; organizaciones, personas, equipamientos, infraestructuras, características geográficas del terreno, fenómenos meteorológicos y medidas de control militares como fronteras, utilizando una aproximación común y extensible de modelado de datos. El núcleo genérico especifica el conjunto mínimo de datos que necesitan ser intercambiados en las operaciones militares conjuntas.

El concepto de núcleo genérico se puede ver en la figura 2, donde se representa el núcleo y distintas áreas funcionales.



**Figura 2**

Cuando el programa MIP se fusionó con ATCCIS y asumió sus objetivos, la nomenclatura varió y el núcleo genérico pasó a llamarse el interfaz común de MIP o MIP Common Interface (MCI).

El MCI modela la información que los comandantes de operaciones conjuntas necesitan intercambiar, esto hace que se pueda cumplir el principal objetivo del programa MIP, es decir, que una fuerza compuesta por una coalición de naciones pueda operar en el moderno espacio de operaciones, de forma sincronizada, como una única fuerza en el cumplimiento de su misión.

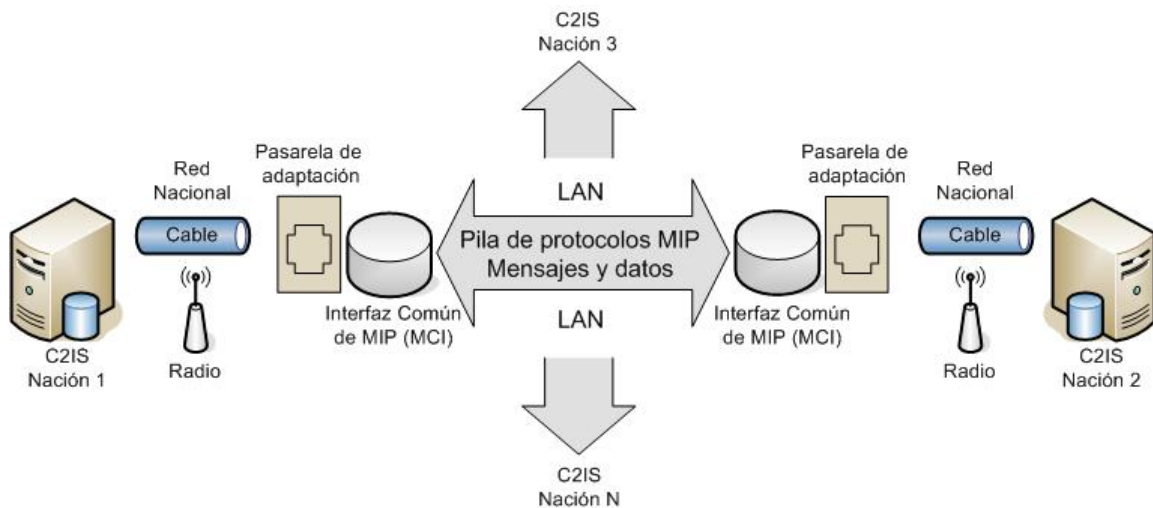
Los MCIs de los distintos países forman la puerta de entrada común a los distintos sistemas de mando y control de los países que forman parte de una determinada operación conjunta, así como a las distintas redes nacionales. La implementación física del MCI es competencia de cada país, este puede formar parte de la base de datos del sistema de mando y control del país o estar en una base de datos separada, lo que implicaría la necesidad de una pasarela de adaptación que mapeara los datos del MCI en la base de datos del sistema de mando y control, de cualquiera de las dos formas, se debe facilitar un idéntico interfaz tanto físico como lógico a los demás sistemas de mando y control, compatibles con MIP, que interoperen en la coalición.

Para facilitar el uso de las redes a todas las naciones participantes en una operación conjunta, cada red o sistema de mando y control debe facilitar una conexión física basada en un estándar muy extendido, las redes de área local Ethernet

Este tipo de redes de área local forman ya parte de los sistemas de mando y control de muchas naciones y por lo tanto se ha extendido su uso para la conexión de los distintos MCIs.

La red de área local Ethernet facilitará la conexión física para dos o más MCIs, por otro lado, cada MCI debe implemententar las funciones de comunicación comunes definidas por MIP para el intercambio de datos entre los sistemas de mando y control de los países aliados.

Un esquema genérico del uso del MCI para facilitar la interoperabilidad entre distintos sistemas de mando y control de países aliados se puede ver en la figura 3.



**Figura 3**

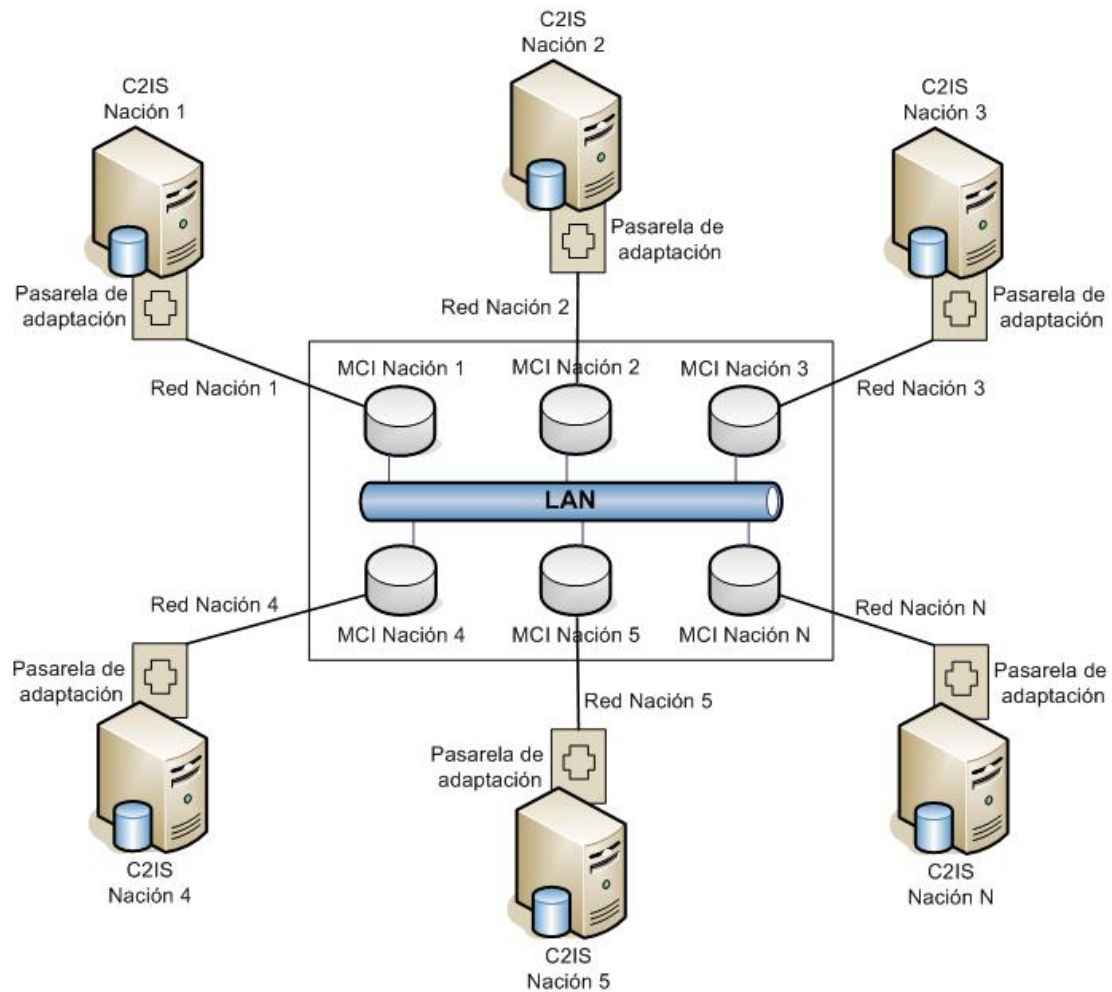
La localización física del MCI dentro de la arquitectura de la red va a depender de la específica topología de red escogida en cada caso.

Tomando como base la arquitectura genérica propuesta por MIP y las funcionalidades que ofrece el MCI a los distintos países participantes en operaciones conjuntas, se van a mostrar diferentes tipos de topologías de red que se pueden implementar dependiendo de las características y requerimientos de cada operación.

La primera topología que se va a describir es la topología de configuración centralizada, en esta topología los distintos MCIs de los países que participan en la coalición están ubicados en una localización centralizada en la que todos los MCIs están interconectados a través de una red de área local sobre la que se han implementado los protocolos y funcionalidades de intercambio de datos diseñados por MIP.

Por el otro extremo cada MCI esta conectado a su sistemas de mando y control a través de cada red nacional. En este caso en que los MCIs no forman parte de la base de datos nativa de casa sistema de mando y control se necesitarán pasarelas de adaptación entre los MCIs de cada país y las bases de datos de su sistema de mando y control.

En la figura 4 se muestra un esquema de la topología centralizada que se acaba de describir.



**Figura 4**

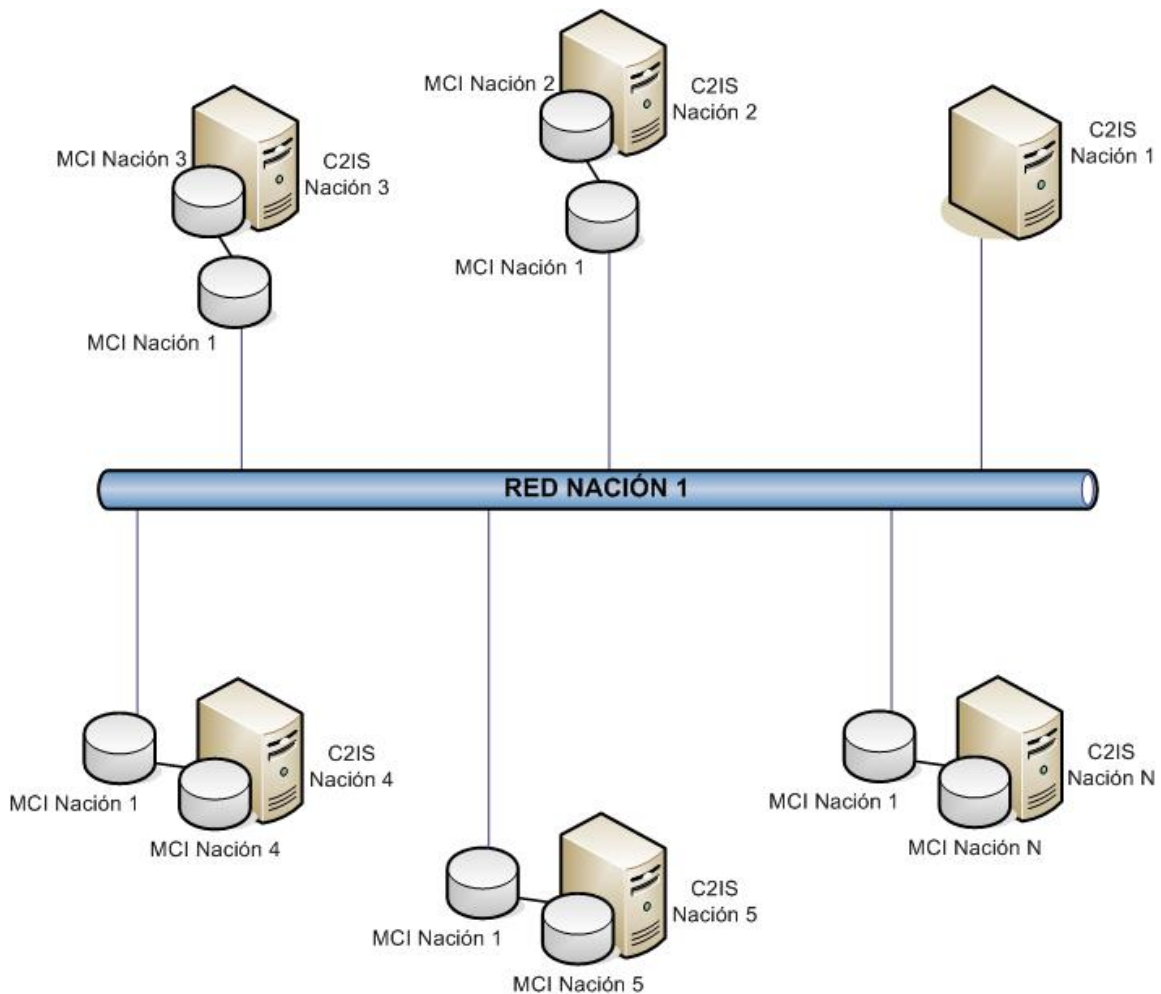
El segundo ejemplo de topología de red que se va a describir en este apartado es la topología descentralizada, en esta topología los MCIs de cada nación forman parte de la base de datos nativa de cada sistema de mando y control, por esta razón las pasarelas de adaptación entre el MCI y la base de datos del sistema de mando y control no son necesarias en esta configuración.

En la topología descentralizada que se describe en el esquema de la figura 5, los MCIs son idénticos a los usados en la configuración centralizada, pero el MCI de cada sistema de mando y control de cada nación está conectado en su propio nodo al MCI de la nación que facilita la red táctica, de esta forma se lleva a cabo la adaptación de cada sistema de mando y control a la red.



Como se puede ver en la figura 5, la nación que facilita la red (Nación 1), no necesita tener su MCI en su nodo, ya que todos los demás nodos tienen una copia del mismo y por lo tanto el intercambio de información entre la base de datos nativa del sistema de mando y control de la nación 1 y su MCI, que en este caso está replicado en cada nodo, es inmediato.

De la misma forma, el intercambio de información entre el MCI de la Nación 1 y los MCIs de las demás naciones es también inmediato y no necesita pasarelas de adaptación, ya que ambos MCIs tienen la misma información estructurada de la misma forma y cumplen los protocolos de intercambio de información diseñados por MIP.



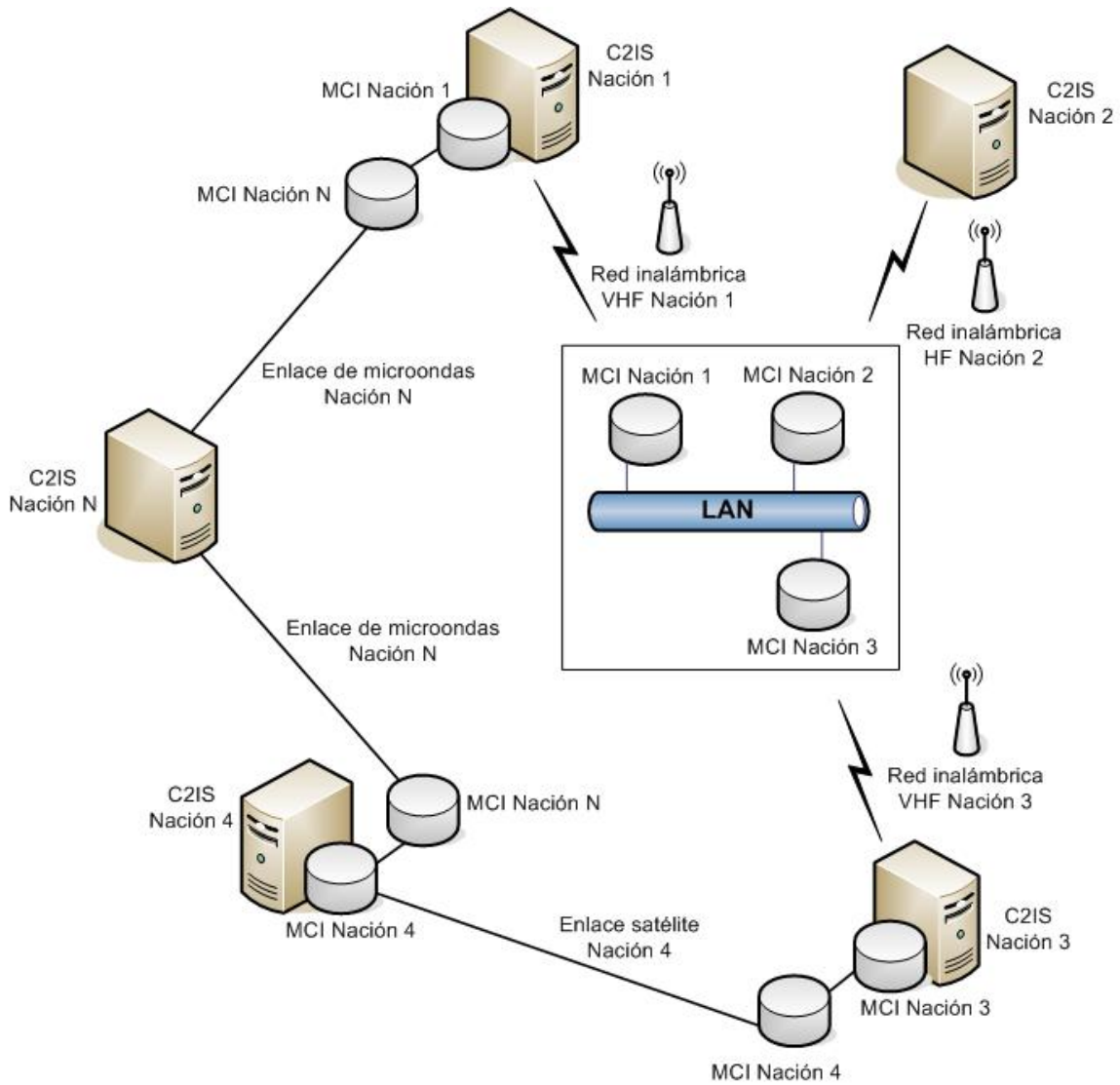
**Figura 5**

En la tercera topología de red que se va a describir se mezclan las dos topologías previamente descritas, la centralizada y la descentralizada, dando lugar a una topología híbrida.

En esta nueva topología de red, al igual que las dos topologías descritas anteriormente, se utiliza los mismos MCIs y las mismas funciones de intercambio de información, solo el direccionamiento de los nodos cambia.

En la figura 6 se puede ver el esquema de una topología de red híbrida, que nos muestra distintas formas de combinación de las redes nacionales de los países aliados utilizando sus MCIs en diferentes configuraciones.

La configuración de una red híbrida puede adaptarse de una forma más sencilla, que en el caso de las configuraciones anteriores, a la naturaleza de la operación conjunta que se va a llevar a cabo



**Figura 6**

Las topologías de red enunciadas en este apartado, describen posibles opciones de despliegue de red que pueden ser usadas por las naciones aliadas en el desarrollo de operaciones conjuntas, dependiendo de la disponibilidad de las redes tácticas en el espacio de operaciones.

Se debe de tener en cuenta, que las distintas especificaciones de seguridad de las naciones participantes en una operación conjunta, pueden afectar a los diferentes despliegues de red descritos anteriormente.

## 2.5 El Land Command and Control Information Exchange Data Model (LC2IEDM)

Como ya se mencionó en el apartado 2.3 de esta tesis doctoral, la primera versión del LC2IEDM fue lanzada dentro del programa ATTCIS el 31 de marzo del 2000, esta versión fue conocida como el LC2IEDM v2. Posteriormente el modelo de datos evolucionó y el 18 de marzo del 2002 se lanzó la siguiente versión del modelo, el LC2IEDM v5. Ambas versiones del modelo de datos LC2IEDM fueron acompañados de sus correspondientes mecanismos de réplica, el ATCCIS Replication Mechanism (ARM) versiones 2 y 5 respectivamente.

Parte del trabajo desarrollado en la presente tesis doctoral ha consistido en la revisión y comparación de alguna de las diferentes versiones de los principales modelos de datos tácticos desarrollados tanto dentro del programa ATTCIS como del programa MIP.

En este apartado se van a describir y a comparar las dos principales versiones del modelo de datos Land Command and Control Information Exchange Data Model (LC2IEDM). Con este trabajo se pretende poner de manifiesto con detalle la evolución del modelo de datos entre ambas versiones.

### 2.5.1 EI LC2IEDM v2

El concepto de “entidad” es básico dentro del modelado de datos [32], con objeto de clarificar el concepto antes de entrar en el análisis de los modelos de datos, se van a dar a continuación algunos ejemplos de posibles entidades. Una entidad puede ser una persona concreta, un lugar, un objeto, un evento o un concepto sobre los que se puede almacenar información. Las propiedades de las distintas entidades dentro del modelo las definen sus atributos, siendo los atributos los datos específicos de cada entidad que son almacenados.

La estructura principal del LC2IEDM v2, que consta de 151 entidades, esta basada en nueve entidades independientes, cinco de las cuales son consideradas clave.

Las cinco entidades clave del LC2IEDM v2 son de una importancia fundamental a la hora de generar la estructura del modelo de datos. Las entidades clave son las siguientes: OBJECT-ITEM, OBJECT-TYPE, CAPABILITY, LOCATION, y ACTION.

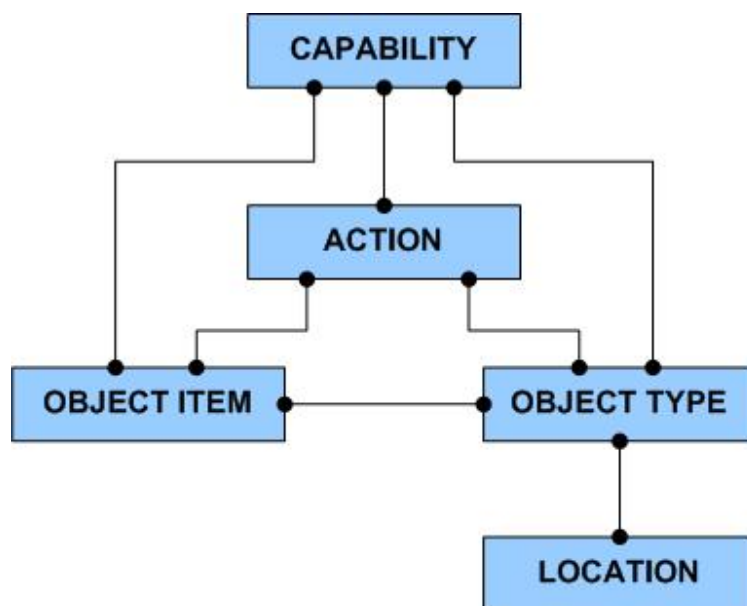
Podemos ver una definición de estas cinco entidades clave del LC2IEDM v2 en la tabla 1.

Entidad Clave	Definición de la entidad	Role en el Modelo
ACTION	Una actividad o la ocurrencia de una actividad que puede utilizar recursos y puede ser focalizada contra un objetivo. Por ejemplo; Orden de operación, plan de operación, orden de movimiento, plan de movimiento, orden de fuego, requerimiento logístico, incidente (ataque enemigo), etc.	Dinámica (Como)
OBJECT-ITEM	Un objeto individualmente identificado que tiene una importancia militar. Por ejemplo; personas individuales, un item material específico, una unidad específica, una característica geográfica específica, etc.	Contenidos (Quien y Que)

OBJECT-TYPE	Una clase de objetos individualmente identificado que tiene una importancia militar. Por ejemplo; un tipo de personas (sargentos), un tipo de material (carros de combate), un tipo de organización (división armada), etc.	
CAPABILITY	La habilidad potencial de realizar algún trabajo, llevar a cabo alguna función o misión, conseguir un objetivo o facilitar un servicio.	
LOCATION	Una especificación de posición y geometría con respecto a una referencia especificada. Por ejemplo; un punto, una secuencia de puntos, una línea poligonal, una elipse, un rectángulo, una esfera o porción, cono, etc. LOCATION especifica ambos localización y dimensiones.	Posicionamiento y formas (Donde)

**Tabla 1. Definición de las cinco entidades clave del LC2IEDM v2 y sus roles.**

Las relaciones entre las cinco entidades clave del modelo LC2IEDM v2 se muestran en la figura 7.



**Figura 7**

Las relaciones que muestra el diagrama de la figura 7 son todas relaciones de “muchos a muchos”, lo que viene indicado por el punto al final de las líneas que indican cada relación.

Este tipo de declaración general de relaciones está permitido por el estándar de modelado IDEF1X [33] solo en diagramas explicativos, como es el caso del diagrama mostrado en la figura 7.

Las restantes entidades independientes del LC2IEDM v2 son las siguientes: CANDIDATE-TARGET-LIST, CONTEXT, REFERENCE, REPORTING-DATA, y RULE-OF-ENGAGEMENT.



La parte superior e inferior del diagrama están conectadas a través de un número de entidades asociadas que se usan para enlazar planes, ordenes y peticiones a través de objetivos, recursos y efectos de OBJECT TYPEs y OBJECT ÍTEMs.

## 2.5.2 EI LC2IEDM v5

La estructura principal del LC2IEDM v5, que consta de 194 entidades, esta basada en doce entidades independientes, nueve de las cuales son consideradas clave.

Las nueve entidades clave del LC2IEDM v5 son de una importancia fundamental a la hora de generar la estructura del modelo de datos. A través de estas nueve entidades clave generan aproximadamente el 77% del modelo de datos, las otras tres entidades independientes generan el 3% del modelo aproximadamente.

El 20% restante del modelo está compuesto por entidades asociativas que interconectan determinadas partes del modelo.

Las entidades clave son las siguientes: OBJECT-ITEM, OBJECT-TYPE, CAPABILITY, LOCATION, REPORTING DATA, CONTEXT, RULE OF ENGAGEMENT, CANDIDATE TARGET LIST y ACTION.

Podemos ver una definición de estas nueve entidades clave del LC2IEDM v5 en la tabla 2.

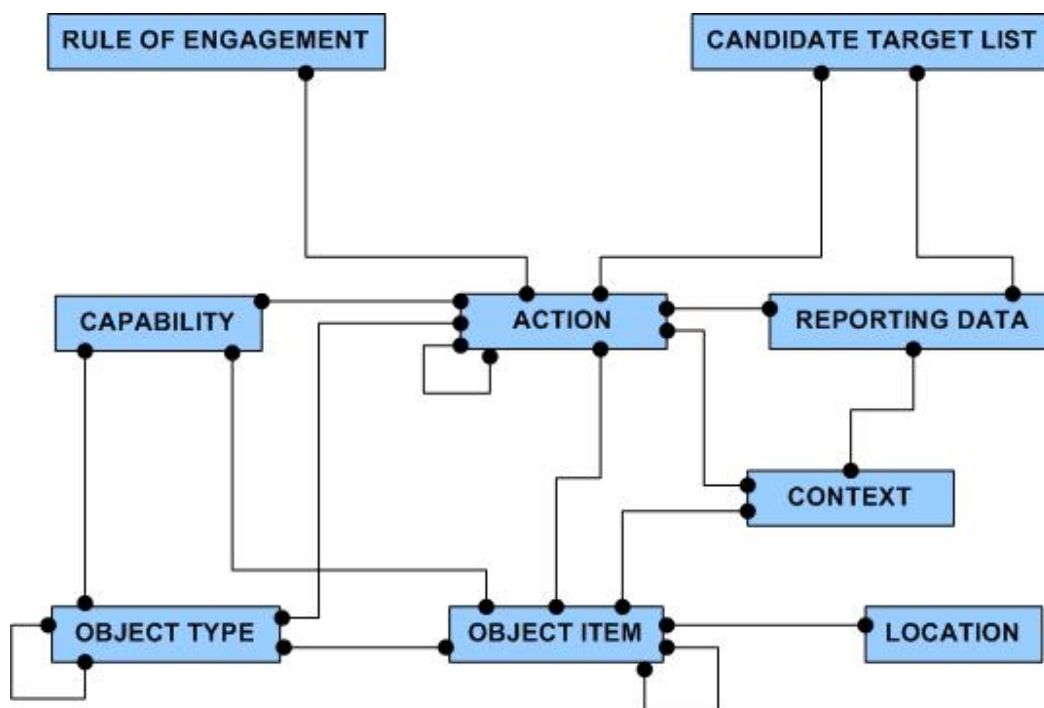
<b>Entidad Clave</b>	<b>Definición de la entidad</b>	<b>Role en el Modelo</b>
ACTION	Una actividad o la ocurrencia de una actividad que puede utilizar recursos y puede ser focalizada contra un objetivo. Por ejemplo; Orden de operación, plan de operación, orden de movimiento, plan de movimiento, orden de fuego, requerimiento logístico, incidente (ataque enemigo), etc.	Dinámica (Como, que, cuando algo va a ser hecho, esta siendo hecho o ha sido hecho)
OBJECT-ITEM	Un objeto individualmente identificado que tiene una importancia militar. Por ejemplo; personas individuales, un item material específico, una unidad específica, una característica geográfica específica, etc.	Identifica cosas (Quien y Que)
OBJECT-TYPE	Una clase de objetos individualmente identificado que tiene una importancia militar. Por ejemplo; un tipo de personas (sargentos), un tipo de material (carros de combate), un tipo de organización (división armada), etc.	Identificación individual de clases de cosas (Quien y Que)
CAPABILITY	La habilidad potencial de realizar algún trabajo, realizar alguna función o misión, conseguir un objetivo o facilitar un servicio.	Indicación de capacidades esperadas para tipos y capacidades actuales de ítems
LOCATION	Una especificación de posición y geometría con respecto a una referencia especificada. Por ejemplo; un punto, una secuencia de puntos, una línea poligonal, una elipse, un rectángulo, una esfera o porción, cono, etc. LOCATION especifica ambos localización y dimensiones.	Posición geográfica de objetos y creación de formas (Donde)
REPORTING-DATA	La especificación de fuente calidad y tiempo que se aplica a unos datos presentados	Apoyo a la función de creación de informes.



CANDIDATE-TARGET-LIST	Una lista de objetos o tipos del espacio de batalla que tengan valor potencial por ser destruidos o explotados. Son nominados por las autoridades competentes para ser considerados en actividades sobre el espacio de batalla.	Información de apoyo a una ACTION
CONTEXT	Una referencia de uno o más REPORTING-DATA	Empaquetado de información
RULE-OF-ENGAGEMENT	Una especificación de unas guías obligatorias para la forma en que una actividad dada es ejecutada.	Apoya a ACTION.

**Tabla 2. Definición de las nueve entidades clave del LC2IEDM v5 y sus roles.**

Las relaciones entre las nueve entidades clave del LC2IEDM v5 se muestran en la figura 9.



**Figura 9**

Las relaciones que muestra el diagrama de la figura 9 son todas relaciones de “muchos a muchos”, lo que viene indicado por el punto al final de las líneas que indican cada relación.

Este tipo de declaración general de relaciones está permitido por el estándar de modelado IDEF1X solo en diagramas explicativos, como es el caso del diagrama mostrado en la figura 9.

Las restantes tres entidades independientes del LC2IEDM v5 son las siguientes: COORDINATE SYSTEM, REFERENCE y VERTICAL DISTANCE.



Estas entidades contienen datos mayoritariamente considerados de categoría estática, principalmente la entidad OBJECT-TYPE. Cabe destacar la relación entre OBJECT-TYPE y OBJECT-ITEM a través de la entidad nueva entidad OBJECT-ITEM-TYPE.

La parte superior e inferior del diagrama están conectadas a través de un número de entidades asociadas que se usan para enlazar planes, ordenes y peticiones a través de objetivos, recursos y efectos de OBJECT TYPEs y OBJECT ÍTEMs.

### **2.5.3 Resumen de la comparación de las versiones del LC2IEDM**

Los principales cambios detectados en la evolución del LC2IEDM, desde su versión 2 publicada el 31 de marzo del 2000, hasta su versión 5 publicada el 18 de marzo del 2002, son los siguientes:

- La versión 5 cuenta con 43 entidades más que la versión 2. Estas 43 nuevas entidades son el fruto de las propuestas de los países participantes en el programa ATCCIS durante los dos años que separan ambas versiones.
- La versión 5 esta basada en 12 entidades independientes 9 de las cuales son consideradas clave, mientras que la versión 2 esta basada en 10 entidades independientes 5 de las cuales son clave.
- El LC2EDM v2 fue el núcleo del modelo de referencia OTAN y fue también la vista del modelo de datos conjunto de la OTAN (STANAG 5523 / AdatP-32). El LC2EDM v5 es presentado en 2002 al grupo de administración de datos de la OTAN como una revisión de esa vista del modelo de datos y con él finaliza la quinta y última fase del programa ATCCIS.

## **2.6 El Command and Control Information Exchange Data Model (C2IEDM)**

Tras la fusión entre los programas MIP y ATTCIS, la evolución del modelo de datos continuó y el 20 de noviembre de 2003, una nueva versión del modelo de datos fue lanzada. A partir de este momento los conceptos no solo se suscribieron al ámbito de las operaciones terrestres y por ello el nuevo modelo de datos perdió la L (Land) y se llamó Command and Control Information Exchange Data Model (C2IEDM) versión 6.1.

Requerimientos operacionales prioritarios hicieron que la versión 6.1 del C2IEDM tuviera que ser modificada, de esta forma el modelo de datos evolucionó y la versión 6.1.5a del C2IEDM fue lanzada el 26 de septiembre de 2004.

Durante 2005 se publicaron 4 nuevas versiones del C2IEDM 6.1.5, a continuación se enumeran estas 4 nuevas versiones y su fecha de publicación;

- El C2IEDM Edition6.15b se publicó el 17 de marzo de 2005.
- El C2IEDM Edition6.15c se publicó el 12 de julio de 2005.
- El C2IEDM Edition6.15d se publicó el 30 de septiembre de 2005.
- El C2IEDM Edition6.15e se publicó el 2 de diciembre de 2005.

En este apartado de la presente tesis doctoral se van a estudiar todas las versiones del C2IEDM, comparándolas entre si, para poder tener una panorámica global de la evolución del modelo de datos.

Este estudio incluye la implementación del esquema físico del C2IEDM Edition6.15c, que como se verá en los capítulos siguientes, formará parte de la investigación que se ha llevado a cabo en esta tesis doctoral.

### 2.6.1 C2IEDM Versión 6.1

Esta versión del modelo de datos, contenía considerablemente más cantidad de contenido orientado al desarrollo de operaciones conjuntas y no solo circunscritas al ámbito terrestre, como resultado de esto el nombre del modelo cambió de L(Land)C2IEDM a C2IEDM en noviembre de 2003.

Como sus versiones previas, el C2IEDM era un modelo de datos para el intercambio de información y en el se especificaba el conjunto mínimo de datos que necesitan ser intercambiados en operaciones multinacionales.

A continuación se describen las características genéricas de la información susceptible de ser intercambiada en un entorno de sistemas de operaciones conjuntas, la mayoría de estas características se heredan de las versiones previas del modelo de datos y se mantendrán en las sucesivas versiones del mismo.

- La estructura de datos debería ser lo suficientemente genérica como para acomodarse a entornos tanto de operaciones de tierra, mar o aire como de operaciones conjuntas.
- El modelo de datos describe todos los objetos de interés en la esfera de operaciones, por ejemplo; organizaciones, personas, equipos, recursos, características geográficas, fenómenos atmosféricos y medidas de control militar como fronteras.
- Los objetos de interés pueden ser genéricos en términos de clase o tipo y específicos en términos de un ítem individualmente identificado. Todos los objetos “ítem” deben ser clasificados como parte de algún objeto “tipo”, por ejemplo un carro de combate individualmente identificado con el número de serie WS62105B es un ítem perteneciente al tipo “Carro de combate de la clase Challenger”.
- Un objeto debe tener la capacidad de llevar a cabo una función o de conseguir un fin. De esta forma se hace necesaria la definición de “capacidad”, para dar significado al valor de los objetos en la esfera de operaciones.
- Debería ser posible poder asignar una localización a cualquier ítem en la esfera de operaciones. Además es necesaria la representación de varias formas geométricas para permitir a los mandos el planificar, dirigir y monitorizar las operaciones, por ejemplo; representación de fronteras, corredores, áreas restringidas, campos de minas, etc.
- Se debe poder mantener o cambiar el estado “status” de cualquier ítem.
- El modelo debe permitir una descripción de un objeto tipo en función de otro objeto tipo. Este concepto incluye tablas de organizaciones, equipamiento o personal.
- El modelo debe reflejar información acerca de lo que es mantenido o poseído en términos de tipos, por un objeto ítem específico.
- Es necesario el almacenar relaciones entre pares de ítems. Serían claves las especificaciones de organizaciones de tareas y ordenes de batalla.

- El modelo debe soportar la especificación del role actual, pasado y futuro de objetos como partes de planes, ordenes y eventos.
- La misma estructura de información debe ser usada para almacenar información de todos los objetos sin tener en cuenta su posible hostilidad.
- Se debe prevenir la identificación de las fuentes de información, los tiempos efectivos de informe y una indicación de la validez de los datos.

La edición 6.1 del C2IEDM contiene 194 entidades, quince de las cuales son independientes, es decir, toda la estructura del modelo de datos está basada en estas quince entidades, el resto de entidades que componen el modelo son entidades dependientes de estas quince.

La definición de las entidades independientes del C2IEDM versión 6.1 así como sus roles se pueden ver en la tabla 3.

Un dato que nos da una idea de la importancia de estas entidades independientes dentro del modelo es que las 5 primeras entidades de esta tabla generan el 82% del modelo de datos, es decir, 159 de las 194 tablas que componen el modelo.

<b>Entidad</b>	<b>Definición de la entidad</b>	<b>Role en el Modelo</b>
ACTION	Una actividad o la ocurrencia de una actividad que puede utilizar recursos y puede ser focalizada contra un objetivo. Por ejemplo; Orden de operación, plan de operación, orden de movimiento, plan de movimiento, orden de fuego, requerimiento logístico, incidente (ataque enemigo), etc.	Dinámica (Como, que, cuando algo va a ser hecho, esta siendo hecho o ha sido hecho)
OBJECT-ITEM	Un objeto individualmente identificado que tiene una importancia militar. Por ejemplo; personas individuales, un item material específico, una unidad específica, una característica geográfica específica, etc.	Identifica cosas o personas individuales (Quien y Que)
OBJECT-TYPE	Una clase de objetos individualmente identificado que tiene una importancia militar. Por ejemplo; un tipo de personas (sargentos), un tipo de material (carro de combate), un tipo de organización (división armada), etc.	Identificación individual de clases (Quien y Que)
CAPABILITY	La habilidad potencial de realizar algún trabajo, realizar alguna función o misión, conseguir un objetivo o facilitar un servicio.	Indicación de capacidades esperadas para tipos y capacidades actuales de ítems
LOCATION	Una especificación de posición y geometría con respecto a una referencia especificada. Por ejemplo; un punto, una secuencia de puntos, una línea poligonal, una elipse, un rectángulo, una esfera o porción, cono, etc. LOCATION especifica ambos localización y dimensiones.	Posición geográfica de objetos y creación de formas (Donde)

ADDRESS	Información precisa de cómo un destino físico o electrónico pueden ser alcanzado o accedido.	Ofrece medios para poder almacenar direcciones postales y electrónicas
AFFILIATION	Una especificación de un país, nacionalidad, grupo étnico, grupo funcional o religión a la cual pertenencia u obediencia pueden ser adscritas.	Ofrece medios para asignar afiliaciones a objetos ítem y a objetos tipo.
CANDIDATE-TARGET-LIST	Una lista de objetos o tipos del espacio de batalla que tengan valor potencial por ser destruidos o explotados. Son nominados por las autoridades competentes para ser considerados en actividades sobre el espacio de batalla.	Información de apoyo a una ACTION
CONTEXT	Una referencia de uno o más REPORTING-DATA	Empaquetado de información
COORDINATE-SYSTEM	Una estructura rectangular de referencia definida por un origen (x,y,z). La coordenada vertical z es tomada de forma perpendicular al plano xy tomando el sentido positivo según la regla de la mano derecha.	Apoya a LOCATION para geometrías relativas específicas.
GROUP-CHARACTERISTIC	Una referencia de un conjunto de características que puede ser utilizada para identificar una colección de objetos distintos. Por ejemplo; grupos de edad, caídos, género y lenguaje clasificación.	Apoya el contado de tipos de personas de acuerdo a unas características seleccionadas.
REFERENCE	Una alusión a una fuente de información que puede tener importancia militar.	Señalar a fuentes de información externas para apoyar a REPORTING-DATA
REPORTING-DATA	La especificación de fuente calidad y tiempo que se aplica a unos datos presentados	Apoyo a la función de creación de informes.
RULE-OF-ENGAGEMENT	Una especificación de unas guías obligatorias para la forma en que una actividad dada es ejecutada.	Apoya a ACTION.
VERTICAL-DISTANCE	Una especificación de la altitud o la altura de un punto o nivel medido con respecto a una referencia dada en la dirección normal al elipsoide de revolución WGS84.	Apoya a LOCATION especificando elevación o altitud.

**Tabla 3. Definición de las entidades independientes del C2IEDM v6.1 y sus roles.**

En la figura 11 se representan todas las entidades independientes definidas anteriormente, con sus correspondientes relaciones.

Las relaciones que muestra el diagrama de la figura 11 son todas relaciones de “muchos a muchos”, lo que viene indicado por el punto al final de las líneas de trazo continuo que indican cada relación. Las relaciones de uno a muchos están indicadas en este diagrama con una línea de trazo discontinuo terminada en un rombo.

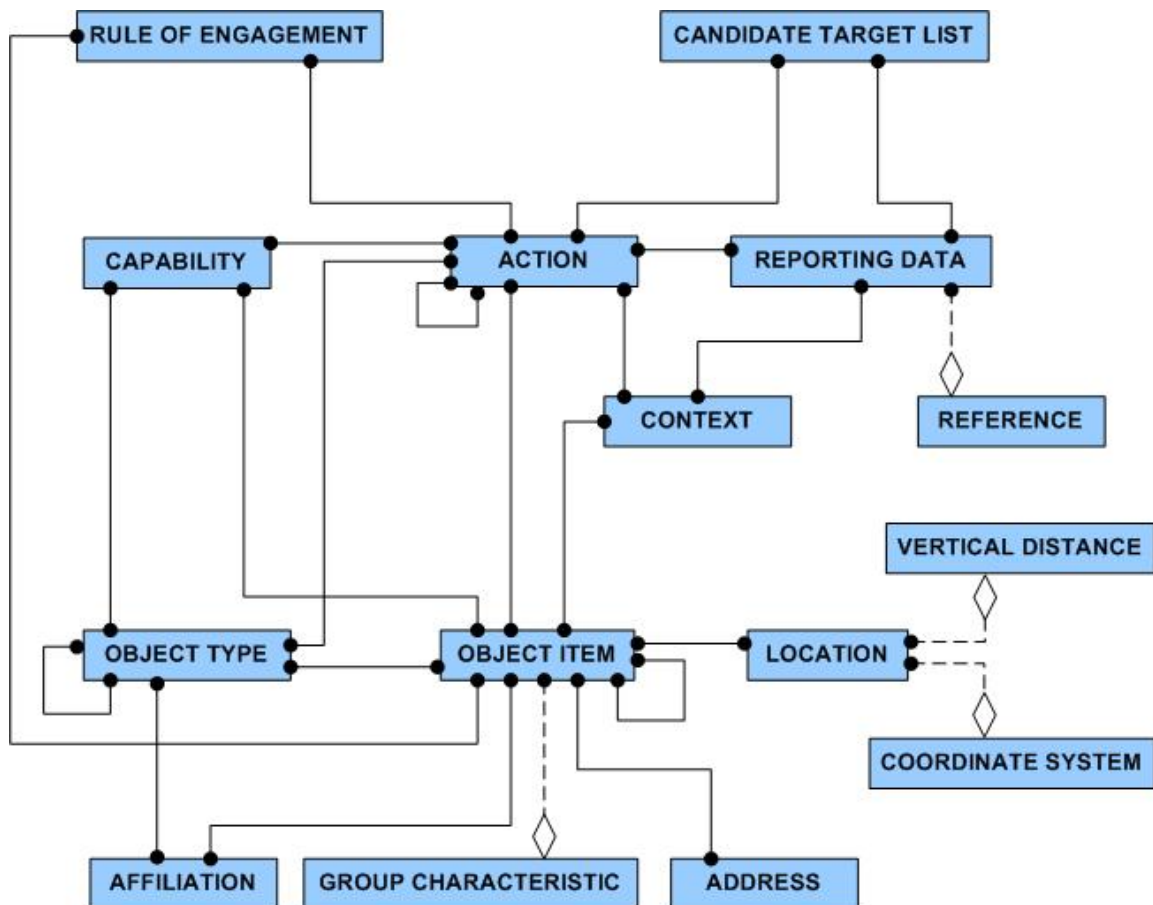


Figura 11

Una visión general del modelo C2IEDM v6.1 se muestra en la figura 12, las quince entidades independientes del C2IEDM v6.1 están sombreadas en color azul. Las relaciones mostradas con líneas de trazos indican relaciones de uno a muchos entre las entidades relacionadas.

Como ya se indicó en las representaciones de la visión general del modelo de anteriores versiones del mismo, el agrupamiento de las entidades en la figura 12 no es casual, con él se pretenden resaltar las siguientes consideraciones.

La parte superior del diagrama está centrada en la entidad ACTION, que esta relacionada con las entidades CAPABILITY, CONTEXT Y RULE-OF-ENGAGEMENT. La naturaleza de estas entidades tiende a ser de naturaleza dinámica, lo cual nos indica; de que son capaces los objetos, como son usados y que objetivos están cumpliendo.

La parte inferior del diagrama se centra en las entidades OBJECT-TYPE, OBJECT-ITEM, y LOCATION lo que va encaminado a un conocimiento de la situación en el espacio de operaciones: que objetos hay en el escenario, que elementos tienen, donde se encuentran, cual es su estado y cuales son sus relaciones con otros objetos del espacio de operaciones. Estas entidades contienen datos mayoritariamente considerados de categoría estática, principalmente la entidad OBJECT-TYPE.



Como en anteriores versiones de este diagrama la parte superior e inferior del diagrama están conectadas a través de un número de entidades asociadas que se usan para enlazar planes, órdenes y peticiones a través de objetivos, recursos y efectos de OBJECT TYPES y OBJECT ÍTEMs.

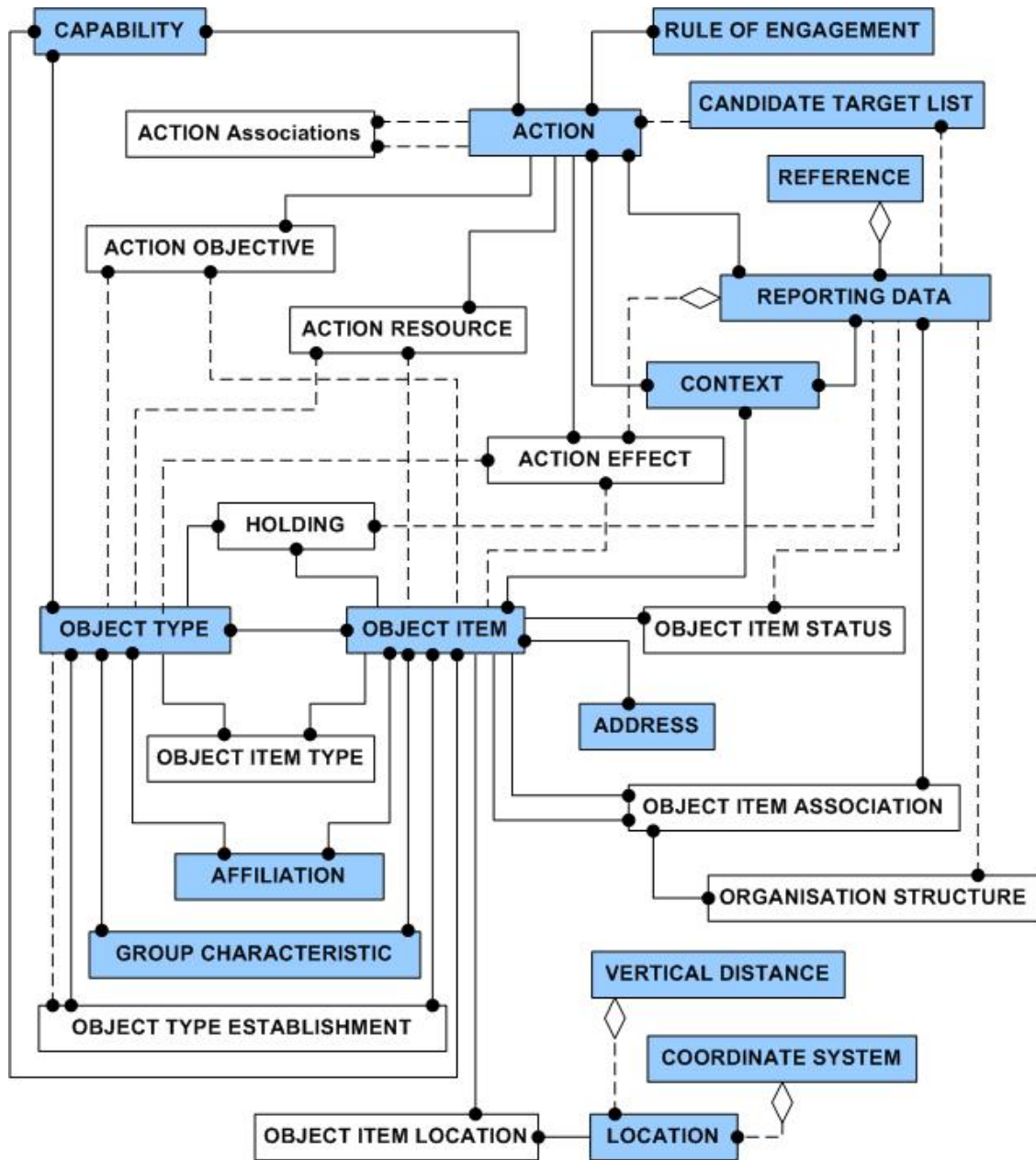


Figura 12

## 2.6.2 C2IEDM Versiones 6.15 (a, b, c, d, e)

En este apartado de la presente tesis doctoral, se van a estudiar las 5 versiones del C2IEDM v6.15. Como ya se ha dicho en apartados anteriores, la aparición de nuevos requerimientos operacionales prioritarios hicieron que la versión 6.1 del C2IEDM tuviera que ser modificada, estos cambios provocaron la evolución del modelo y la versión 6.1.5a del C2IEDM se publicó el 26 de septiembre de 2004.

Durante 2005 se publicaron 4 nuevas versiones del C2IEDM 6.1.5, cada una incluía pequeños cambios estructurales. El hecho de que las cinco versiones del C2IEDM tengan solo pequeñas diferencias entre ellas, ha hecho que en este apartado se haya decidido estudiarlas y compararlas de forma conjunta y no una por una, ya que al ser sus estructuras muy similares, la repetición de su descripción y diagramas para cada versión del modelo sería muy repetitivo y poco clarificador.

Por ello en la primera parte de este apartado se analizarán y compararán las 5 versiones del modelo C2IEDM v6.15 y posteriormente, en los siguientes apartados de la presente tesis se describirá la implementación del esquema físico del C2IEDM v6.15c, que servirá como elemento representativo del modelo de datos C2IEDM v6.15.

### 2.6.2.1 Análisis de las diferentes versiones del modelo C2IEDM v6.15

La **versión 6.15a** del C2IEDM está compuesta por 202 entidades, 6 más que el C2IEDM v6.1, y 1426 atributos. La estructura completa de la versión 6.15a del modelo de datos se genera a partir de 15 entidades independientes.

Las 15 entidades independientes de la versión v6.15a del C2IEDM coinciden con las entidades independientes del C2IEDM v6.1 y son las siguientes: ACTION, OBJECT-ITEM, OBJECT-TYPE, CAPABILITY LOCATION, ADDRESS, AFFILIATION, CANDIDATE-TARGET-LIST, CONTEXT, COORDINATE-SYSTEM, GROUP-CHARACTERISTIC, REFERENCE, REPORTING-DATA, RULE-OF-ENGAGEMENT, VERTICAL-DISTANCE.

Las relaciones entre las entidades independientes de la versión v6.15a del C2IEDM coinciden con las relaciones de las entidades independientes de la versión 6.1 del C2IEDM. Ver figura 11.

La **versión 6.15b** del C2IEDM está compuesta por 203 entidades, una más que la versión 6.15a, y 1433 atributos. La nueva entidad que incorpora la versión 6.15b es ACTION-LOCATION y sus 7 atributos, son los 7 atributos de más con los que cuenta la versión 6.15b del C2IEDM con respecto a la versión 6.15a.

La estructura completa de la versión 6.15b del modelo de datos se genera a partir de 15 entidades independientes. Las 15 entidades independientes de la versión v6.15b del C2IEDM coinciden con las entidades independientes de la versión 6.15a del C2IEDM.

Las relaciones entre las entidades independientes de la versión v6.15b del C2IEDM también coinciden, como en el caso de la versión 6.15a, con las relaciones de las entidades independientes de la versión 6.1 del C2IEDM. Ver figura 11.

La nueva entidad que incorpora la versión 6.15b, ACTION-LOCATION, se define como una asociación de una instancia de la entidad ACTION con una instancia de la entidad LOCATION, lo que permite el posicionamiento geográfico directo de dicha acción, así como el poder disponer de un histórico de las distintas posiciones en las que se desarrolla una acción determinada.

La estructura completa de la entidad ACTION-LOCATION con todas sus relaciones se puede ver en la figura 13.

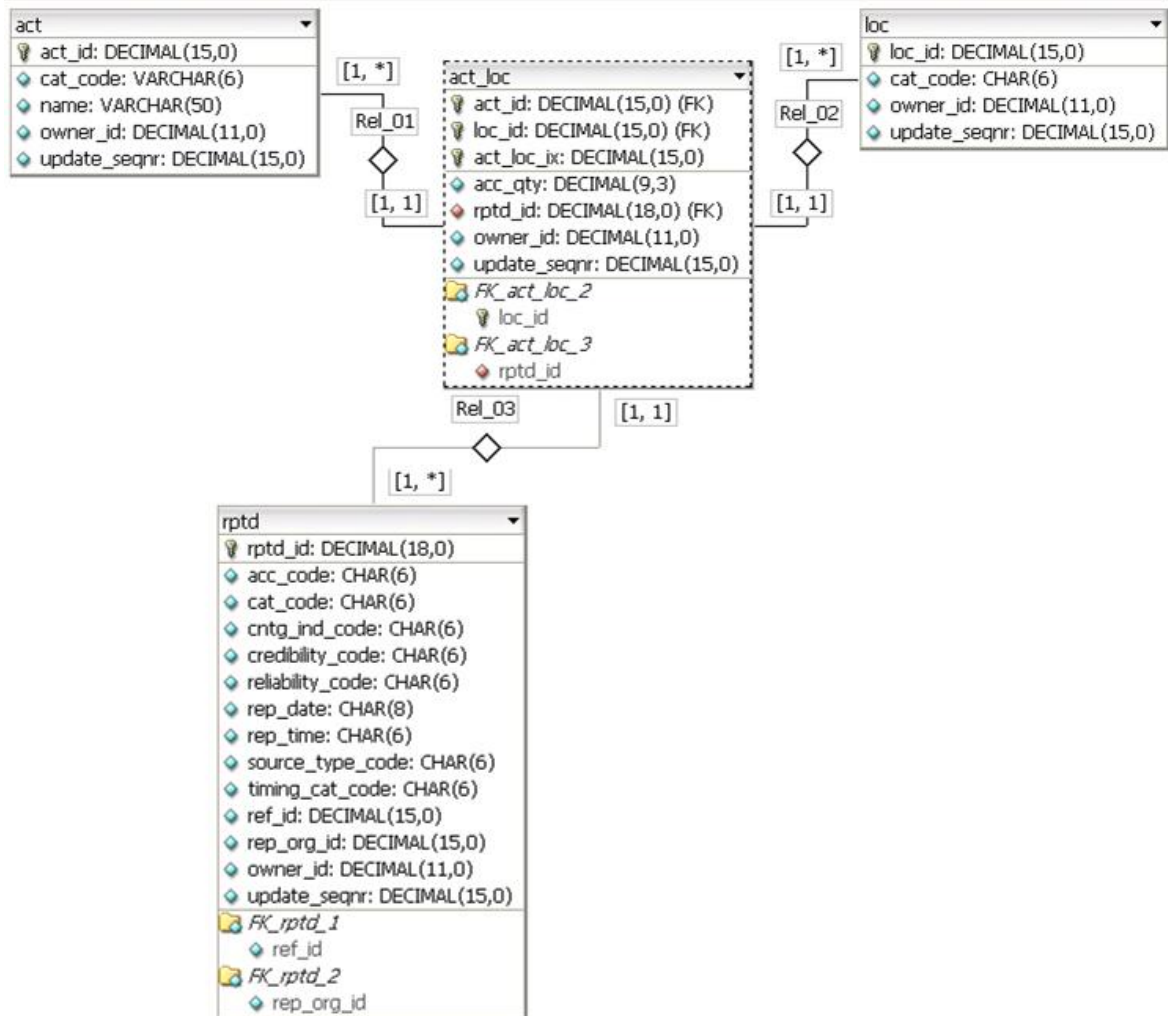


Figura 13

La entidad ACTION-LOCATION también está relacionada con REPORTING-DATA mediante una relación de 1:n, esta relación permite adjuntar cualquier información que esté dentro de la estructura de REPORTING-DATA a una instancia de la entidad ACTION-LOCATION.

La **versión 6.15c** del C2IEDM está compuesta por 203 entidades y 1433 atributos, al igual que la versión 6.15b. La estructura completa de la versión 6.15c del modelo de datos se genera a partir de 15 entidades independientes. Las 15 entidades independientes de la versión v6.15c del C2IEDM coinciden con las entidades independientes de la versión 6.15b del C2IEDM.

Las relaciones entre las entidades independientes de la versión v6.15c del C2IEDM también coinciden, como en el caso de la versión 6.15b, con las relaciones de las entidades independientes de la versión 6.1 del C2IEDM. Ver figura 11.

La nueva característica que incorpora la versión 6.15c del modelo de datos, con respecto a la 6.15b es la forma de definición, representación geométrica y almacenamiento de los datos que definen las fronteras entre las distintas unidades militares que componen un contingente.

En la figura 14 podemos ver un ejemplo de la definición y representación de las fronteras entre las unidades que componen un contingente de tropas que se proponían en la versión 6.15b del C2IEDM.

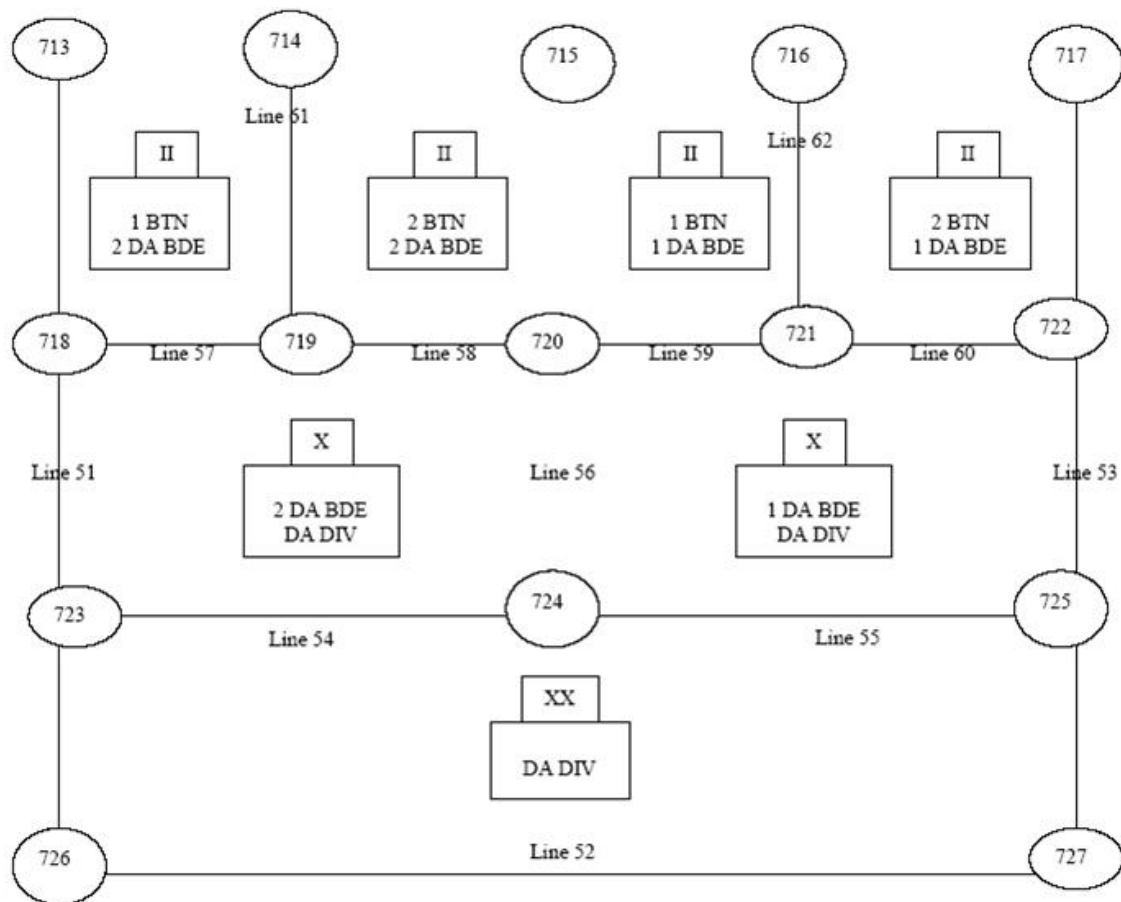


Figura 14

En la figura 15 podemos ver un ejemplo de la definición y representación de las fronteras entre las unidades que componen un contingente de tropas que se propone en la versión 6.15c del C2IEDM.

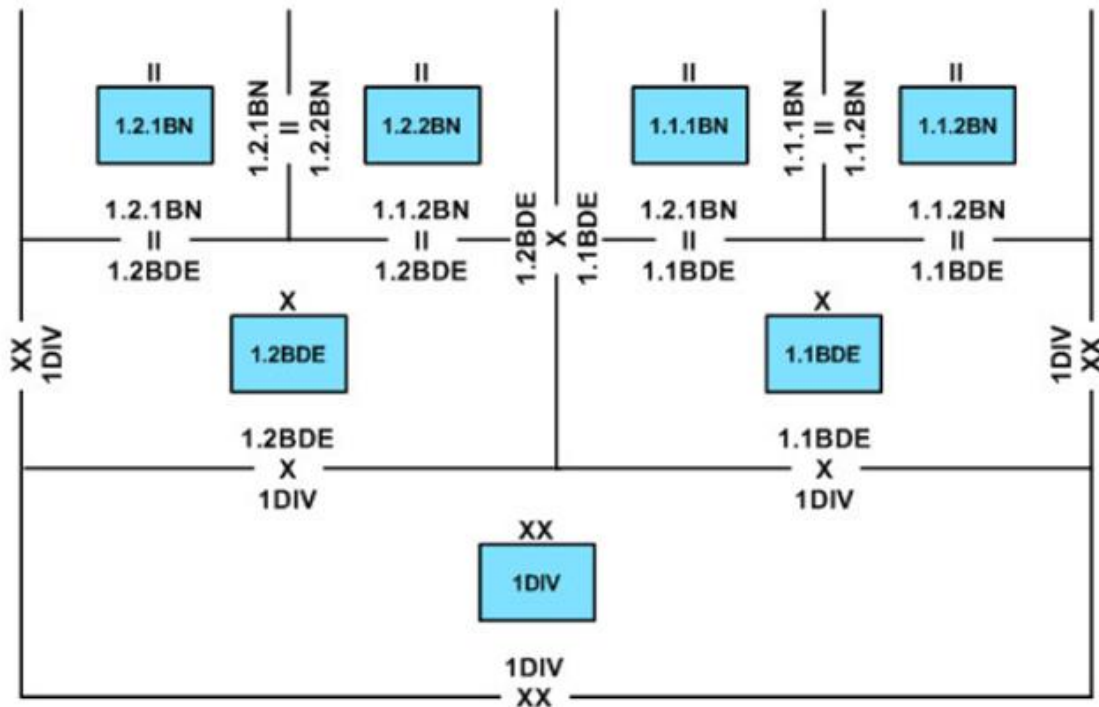


Figura 15

La **versión 6.15d** del C2IEDM está compuesta por 203 entidades y 1433 atributos, al igual que la versión 6.15c. La estructura completa de la versión 6.15d del modelo de datos se genera a partir de 15 entidades independientes. Las 15 entidades independientes de la versión v6.15d del C2IEDM coinciden con las entidades independientes de la versión 6.15c del C2IEDM.

Las relaciones entre las entidades independientes de la versión v6.15d del C2IEDM también coinciden, como en el caso de la versión 6.15c, con las relaciones de las entidades independientes de la versión 6.1 del C2IEDM. Ver figura 11.

Las diferencias detectadas entre las versiones 6.15c y 6.15d son mínimas, hemos de tener en cuenta que una versión se publicó en julio del 2005 y la siguiente en septiembre del mismo año.

Estas diferencias se circunscribirían a algunos cambios puntuales en la descripción de los datos que representan algunos atributos, un ejemplo de estos cambios puntuales podría ser el atributo 5 de la entidad CLOUD-COVER.

Este atributo se define como un número de 6 cifras enteras y 3 cifras decimales en la versión 6.15c del modelo de datos y como un número de 7 cifras enteras y 7 cifras decimales en la versión 6.15d.

La **versión 6.15e** del C2IEDM está compuesta por 203 entidades y 1434 atributos, uno más que la versión 6.15d, este atributo nuevo se añadió a la entidad ORGANISATION-STRUCTURE, concretamente se trata del atributo: *organisation-structure-name*. Algunas nuevas reglas de utilización de la información, como es el caso del uso de la entidad REPORTING-DATA-ABSOLUTE-TIMINIG, han sido actualizadas aunque esto no provocó cambios en el modelo.

La estructura completa de la versión 6.15e del modelo de datos se genera a partir de 15 entidades independientes. Las 15 entidades independientes de la versión v6.15e del C2IEDM coinciden con las entidades independientes de la versión 6.15d del C2IEDM.

Las relaciones entre las entidades independientes de la versión v6.15e del C2IEDM también coinciden, como en el caso de la versión 6.15d, con las relaciones de las entidades independientes de la versión 6.1 del C2IEDM. Ver figura 11.

Como ocurrió en el caso de la comparación entre las versiones 6.15c y 6.15d, el hecho de que el periodo de tiempo transcurrido entre la publicación de la versión 6.15d y la 6.15e fuera solo de dos meses hace que los cambios introducidos en la nueva versión sean mínimos con respecto a su predecesora.

## **2.7 Joint Consultation Command and Control Information Exchange Data Model (J3CIEDM)**

Como ya se mencionó en el apartado 2.3 de esta tesis doctoral, la primera versión del J3CIEDM fue lanzada el 10 de diciembre del 2004, esta versión fue conocida como el J3CIEDM Ed 0.5. Posteriormente el modelo de datos evolucionó y el 9 de diciembre del 2005 se lanzó la siguiente versión del modelo, el J3CIEDM Ed 3.0. La última edición del J3CIEDM es la 3.1 que se publicó el 8 de diciembre del 2006.

Siguiendo con el trabajo de revisión y comparación de alguna de las diferentes versiones de los principales modelos de datos tácticos desarrollados tanto dentro del programa ATTCIS como del programa MIP, en este apartado se van a describir y a comparar las dos versiones del modelo de datos Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM) publicadas hasta el momento.

Con este trabajo se pretende poner de manifiesto con detalle la evolución del modelo de datos entre ambas versiones y en capítulos posteriores se describirá la implementación del esquema físico del J3CIEDM Ed 3.0, que se ha llevado a cabo como parte de la investigación desarrollada en la presente tesis doctoral y que servirá como elemento representativo del modelo J3CIEDM.

### **2.7.1 El JC3IEDM Ed 3.0**

El modelo JC3IEDM es el resultado de la convergencia de los requerimientos operacionales propuestos por NATO/ACT y el grupo de operaciones de MIP. Estos requerimientos cubren necesidades centradas en Air Tasking Order (ATO), temas relacionados con asuntos de naturaleza química, biológica, radiológica y nuclear (Chemical, Biological, Radiological and Nuclear, CBRN) y los mensajes relacionados con uso de minas marítimas.

La edición 3.0 del Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM) esta compuesta por 241 entidades y 1729 atributos, 38 entidades y 295 atributos más que la versión 6.15e del modelo C2IEDM, que fue publicada el 2 de diciembre de 2005, solo 7 días antes que la publicación del JC3IEDM Ed 3.0. Este hecho nos indica que tanto el C2IEDM v6.15 como el J3CIEDM han llevado desarrollos paralelos, ya que el JC3IEDM Ed 3.0 no es la evolución directa del C2IEDM v6.15e, sino que como se dijo en el apartado 2.3 de esta tesis doctoral, el JC3IEDM Ed 3.0 es una evolución del J3CIEDM Ed 0.5 que a su vez es el fruto de la fusión de la versión 4 del GH y el C2IEDM v6.1.

La estructura completa del JC3IEDM se genera a partir de 15 entidades independientes, estas entidades independientes y sus relaciones coinciden con las entidades independientes del modelo C2IEDM v6.15e y sus versiones anteriores y pueden verse en apartados anteriores de la presente tesis doctoral.

Las nuevas entidades incluidas en el JC3IEDM Ed 3.0 y que no se encontraban en el C2IEDM v6.15e son 41, el hecho de que el JC3IEDM Ed 3.0 solo tenga 38 entidades más que C2IEDM v6.15e se debe a que las entidades MASS-GRAVE, MASS-GRAVE-CONTENT y AFFILIATION-EXERCISE-GROUP, que se podían encontrar en el C2IEDM v6.15e, no parecen en el esquema físico del JC3IEDM Ed 3.0.

Las 41 nuevas entidades que incorpora el JC3IEDM Ed 3.0 en relación al C2IEDM v6.15e han sido identificadas y son las siguientes:

ACTION-OBJECTIVE-TASK, ACTION-REFERENCE-ASSOCIATION, ACTION-RECONNAISSANCE-EMPLOYMENT, ACTION-OBJECTIVE-TYPE-IMAGERY-PRODUCT, ACTION-ELECTRONIC-WARFARE-EMPLOYMENT, AIRFIELD-STATUS, AIRFIELD-TYPE, AIRSPACE-CONTROL-MEANS, AIR-ROUTE-SEGMENT, APPROACH-DIRECTION, APRON, CHEMICAL-BIOLOGICAL-EVENT, CARTESIAN-POINT, CAPABILITY-REFERENCE-ASSOCIATION, GEOGRAPHIC-POINT, HARBOUR-TYPE, LIQUID-SURFACE-STATUS, MARITIME-EQUIPMENT-TYPE, MINEFIELD-LAND, MINEFIELD-MARITIME, MINEFIELD-MARITIME-CASUALTY-ESTIMATE, MINEFIELD-MARITIME-SUSTAINED-THREAT-MEASURE-OF-EFFECTIVENESS, NETWORK-SERVICE-STATUS, NUCLEAR-EVENT, NUCLEAR-WEAPON-EVENT, OBJECT-ITEM-REFERENCE-ASSOCIATION, OBJECT-TYPE-REFERENCE-ASSOCIATION, ORGANISATION-REFERENCE-ASSOCIATION, OBJECT-ITEM-ALIAS, RADIOACTIVE-EVENT, RADIOLOGICAL-EVENT, RAILWAY, REFERENCE-ASSOCIATION, ROAD, ROUTE-SEGMENT, ROUTE-TYPE, RUNWAY, RUNWAY-APPROACH-DIRECTION-ASSOCIATION, SOLID-SURFACE-STATUS, SURFACE-VESSEL-TYPE, SUBSURFACE-VESSEL-TYPE

Además de las nuevas entidades incorporadas en el JC3IEDM Ed 3.0 en respuesta a requerimientos relacionados con operaciones aéreas, mejora de las especificaciones de la entidad ACTION, temas relacionados con CBRN (Chemical, Biological, Radiological and Nuclear) se da un refinamiento de las estructuras jerárquicas dentro del modelo. Se han renombrado numerosas entidades por cambios en la estructura del modelo de datos, por ejemplo, en el C2IEDM V6.15e la entidad HARBOUR era una entidad dependiente de la entidad FACILITY y a su vez de ella dependían otras 7 entidades.

En el J3CIEDM estas 7 unidades ya no dependen directamente de la entidad HARBOUR sino que han pasado a depender directamente de la entidad FACILITY, quedando por lo tanto al mismo nivel que HARBOUR, por este cambio estructural las 7 entidades han sido renombradas.

En la tabla 4 se pueden ver las entidades a las que se hace referencia en el párrafo anterior tanto con el nombre que tenían en el C2IEDM como con el nombre con el que aparecen en el J3CIEDM Ed.3.0.

Nombre de la entidad en el C2IEDM	Nombre de la entidad en el J3CIEDM Ed 3.0
HARBOUR ANCHORAGE	ANCHORAGE
HARBOUR BASIN	BASIN
HARBOUR BERTH	BERTH
HARBOUR DRY DOCK	DRY DOCK
HARBOUR JETTY	JETTY
HARBOUR QUAY	QUAY
HARBOUR SLIPWAY	SLIPWAY

**Tabla 4 Entidades renombradas en el J3CIEDM por cambios estructurales**



De la misma forma, otras entidades del modelo C2IEDM v6.15e han sido renombradas por requerimientos de naturaleza CBRN (Chemical, Biological, Radiological and Nuclear) en el J3CIEDM Ed. 3.0.

Estas entidades renombradas son 5 y se pueden ver en la tabla 5.

Nombre de la entidad en el C2IEDM	Nombre de la entidad en el J3CIEDM Ed 3.0
BIOLOGICAL-AGENT-TYPE	BIOLOGICAL-MATERIEL-TYPE
CHEMICAL-AGENT-TYPE	CHEMICAL-MATERIEL-TYPE
LAND-WEAPON-TYPE	WEAPON-TYPE
MEDICAL-FACILITY-STATUS-CASUALTY-EVACUATION	MEDICAL-FACILITY-STATUS-PENDING-CASUALTY-EVACUATION
NBC-EQUIPMENT-TYPE	CBRN-EQUIPMENT-TYPE
NBC-EVENT	CBRN-EVENT

**Tabla 5 Entidades renombradas en el J3CIEDM por requerimientos CBRN**

En la nomenclatura de los atributos de las entidades, algunas de sus palabras clase han sido modificadas en el J3CIEDM, podemos ver los cambios en palabras clase del modelo en la tabla 6.

Palabra clase en el C2IEDM v6.15e	Palabra clase en el J3CIEDM Ed.3.0
DATE DATETIME	FRACTION RATIO
NAME TEXT	TIME DATETIME
DATE DATETIME	FRACTION RATIO
NAME TEXT	TIME DATETIME
QUANTITY COUNT	QUANTITY ORDINAL
QUANTITY COUNT	QUANTITY ORDINAL
No existía	AMOUNT
No existía	BINARY OBJECT

**Tabla 6 Cambios en las palabras clase de los atributos en el J3CIEDM Ed.3.0**

## 2.7.2 El JC3IEDM Ed 3.1

La edición 3.1 del JC3IEDM fue publicada el 8 de diciembre de 2006 y es una evolución directa de la edición 3.0 del mismo modelo, que se ha descrito en el apartado anterior, en este apartado se pondrán de manifiesto las principales diferencias entre las dos ediciones.

El JC3IEDM edición 3.1 contiene 271 entidades y 2005 atributos, 30 entidades y 276 atributos más que la edición 3.0 del J3CIEDM.

La estructura completa del JC3IEDM edición 3.1 se genera a partir de 19 entidades independientes, 4 más que en la versión anterior.

Debido al hecho de que el número y algunos nombres y definiciones de las entidades independientes de la versión 3.1 del J3CIEDM han variado con respecto a las de su versión anterior y por lo tanto también han variado con respecto al C2IEDM v6.15e, en el presente apartado se van a describir las 19 entidades independientes de la edición 3.1 del modelo J3CIEDM.

En la tabla 7 se pueden ver las 19 entidades independientes que generan el J3CIEDM así como sus definiciones.

<b>Entidad</b>	<b>Definición de la entidad</b>	<b>Role en el Modelo</b>
ACTION	Una actividad o la ocurrencia de una actividad que puede utilizar recursos y puede ser focalizada contra un objetivo. Por ejemplo; Orden de operación, plan de operación, orden de movimiento, plan de movimiento, orden de fuego, requerimiento logístico, incidente (ataque enemigo, inicio de una misión), etc.	Dinámica (Como, que, cuando algo va a ser hecho, esta siendo hecho o ha sido hecho)
OBJECT-ITEM	Un objeto individualmente identificado que tiene una importancia militar. Por ejemplo; personas individuales, un ítem material específico, una unidad específica, una característica geográfica específica, etc.	Identifica cosas o personas individuales (Quien y Que)
OBJECT-TYPE	Una clase de objetos individualmente identificado que tiene una importancia militar. Por ejemplo; un tipo de personas (sargentos), un tipo de material (carro de combate), un tipo de organización (división armada), etc.	Identificación individual de clases (Quien y Que)
CAPABILITY	La habilidad potencial de realizar algún trabajo, realizar alguna función o misión, conseguir un objetivo o facilitar un servicio.	Indicación de capacidades esperadas para tipos y capacidades actuales de ítems

LOCATION	Una especificación de posición y geometría con respecto a una referencia especificada. Por ejemplo; un punto, una secuencia de puntos, una línea poligonal, una elipse, un rectángulo, una esfera, cono, etc. LOCATION especifica ambos localización y dimensiones.	Posición geográfica de objetos y creación de formas (Donde)
ADDRESS	Información precisa de cómo un destino físico o electrónico pueden ser alcanzado o accedido.	Ofrece medios para poder almacenar direcciones postales y electrónicas
AFFILIATION	Una especificación de un país, nacionalidad, grupo étnico, grupo funcional o religión a la cual pertenencia u obediencia pueden ser adscritas.	Ofrece medios para asignar afiliaciones a objetos ítem y a objetos tipo.
CANDIDATE-TARGET-LIST	Una lista de objetos o tipos del espacio de batalla que tengan valor potencial por ser destruidos o explotados. Son nominados por las autoridades competentes para ser considerados en actividades sobre el espacio de batalla.	Información de apoyo a una ACTION
CONTEXT	Una referencia de uno o más REPORTING-DATA	Empaquetado de información
RELATIVE-COORDINATE-SYSTEM	Una estructura rectangular de referencia definida por un origen (x,y,z). La coordenada vertical z es tomada de forma perpendicular al plano xy tomando el sentido positivo según la regla de la mano derecha.	Apoya a LOCATION para geometrías relativas específicas.
GROUP-CHARACTERISTIC	Una referencia de un conjunto de características que puede ser utilizada para identificar una colección de objetos distintos. Por ejemplo; grupos de edad, caídos, género y lenguaje clasificación.	Apoya el contado de tipos de personas de acuerdo a unas características seleccionadas.
REFERENCE	Una alusión a una fuente de información que puede tener importancia militar.	Señalar a fuentes de información externas como apoyo de REPORTING-DATA
REPORTING-DATA	La especificación de fuente calidad y tiempo que se aplica a unos datos presentados	Apoyo a la función de creación de informes.
RULE-OF-ENGAGEMENT	Una especificación de unas guías obligatorias para la forma en que una actividad dada es ejecutada.	Apoya a ACTION.

VERTICAL-DISTANCE	Una especificación de la altitud o la altura de un punto o nivel medido con respecto a una referencia dada en la dirección normal al elipsoide de revolución WGS84.	Apoya a LOCATION especificando elevación o altitud.
COMPONENT-HEADER-CONTENT	Asunto introductorio que identifica un elemento, una orden o un plan.	Usado conjuntamente con las especificaciones de planes y órdenes.
COMPONENT-TEXT-CONTENT	Una declaración textual de un asunto considerado importante.	Usado conjuntamente con las especificaciones de planes y órdenes.
PLAN-ORDER	Un esquema planeado u ordenado llevado a cabo previamente para el cumplimiento de un objetivo operacional.	Entidad de alto nivel para la identificación de un plan o una orden.
SECURITYCLASSIFICATION	La clasificación de seguridad aplicable a una fuente de información dentro del dominio de información clasificada.	Apoyo a las entidades CONTEXT, NETWORK-SERVICE y REFERENCE

**Tabla 7. Definición de las entidades independientes del J3CIEDM Ed 3.1**

En la figura 16 se representan todas las entidades independientes definidas anteriormente, con sus correspondientes relaciones.

Las relaciones que muestra el diagrama de la figura 16 son todas relaciones de “muchos a muchos”, lo que viene indicado por el punto al final de las líneas de trazo continuo que indican cada relación. Las relaciones de uno a muchos están indicadas en este diagrama con una línea de trazo discontinuo terminada en un rombo.

Este tipo de declaración general de relaciones está permitido por el estándar de modelado IDEF1X solo en diagramas explicativos, como es el caso del diagrama mostrado en la figura 16.

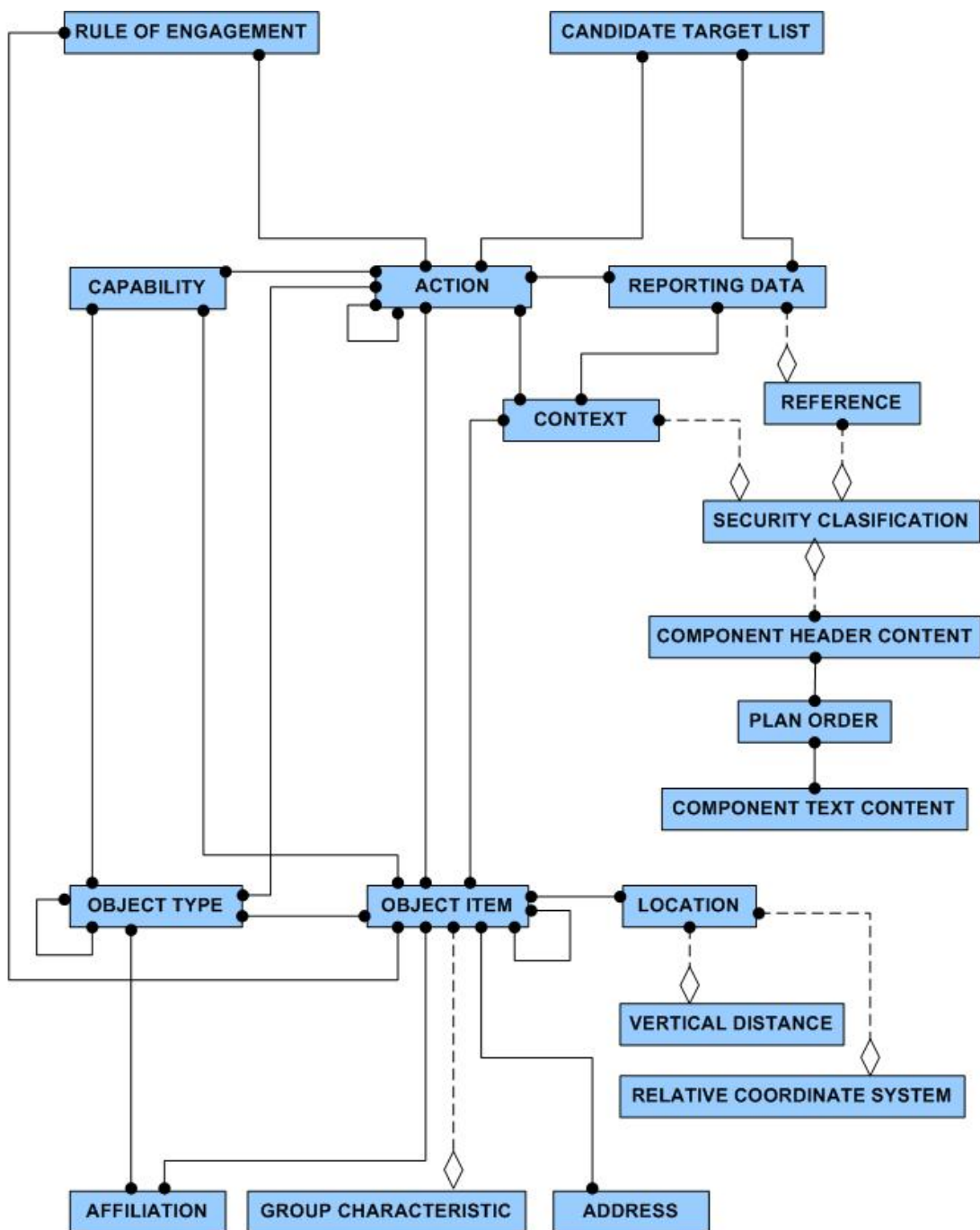


Figura 16

Una vez se han descrito los cambios en las entidades independientes que presenta la versión 3.1 del modelo se va a pasar a describir con detalle los cambios estructurales y nuevas incorporaciones de entidades al modelo.

En los siguientes párrafos se resumirán los principales cambios sufridos por el modelo y las razones que los han motivado.

Los principales cambios a nivel de entidad (adición, cambios y borrado de entidades) han ocurrido en las áreas de ACTION-RESOURCE-EMPLOYMENT, CAPABILITY, HOLDING, OBJECT-ITEM-HOSTILITY-STATUS, OBJECT-ITEM-STATUS, SECURITY CLASSIFICATION y Planificación y Ordenes. Los detalles de estos cambios van a ser descritos a continuación.

En la estructura de la entidad ACTION-RESOURCE-EMPLOYMENT se añadió la entidad ACTION-MARITIME-EMPLOYMENT para apoyar el empleo de recursos marítimos. A las restantes entidades de la estructura se les añadieron algunos atributos con objeto de apoyar los requerimientos de la ordenación de tareas aéreas.

La estructura completa de la entidad CAPABILITY fue cambiada al añadirle 4 nuevas entidades; HANDLING, MAINTENANCE, SUPPORT y TRANSMISSION. El nombre de la entidad MISSION-CAPABILITY fue cambiado por OPERATIONAL-CAPABILITY. El resto de entidades de la estructura de la entidad CAPABILITY sufrieron cambios en los nombres de algunos de sus atributos para gestionar los nuevos requerimientos identificados.

La entidad HOLDING-TRANSFER fue añadida a la estructura de la entidad HOLDING para permitir la adición o el borrado de cantidades tipo a unidades holding específicas.

En la entidad OBJECT-ITEM-HOSTILITY-STATUS se eliminó el atributo “object item status hostility code”, de esta forma se permitió a las naciones el dar un estado de hostilidad a un objeto OBJECT-ITEM sin tener que especificar ningún otro atributo de estado.

La estructura de la entidad OBJECT-ITEM-STATUS se cambió al añadirle 3 nuevas entidades LIQUID-BODY-STATUS, MINEFIELD-MARITIME-STATUS y MINE-STATUS.

En la estructura de la entidad OBJECT-ITEM se añadió una la entidad INSTRUMENT-LANDING-SYSTEM para apoyar los requerimientos de la ordenación de tareas aéreas.

Se añadió al modelo la entidad SECURITY-CLASSIFICATION, lo que permitió que los atributos dedicados a la clasificación de seguridad de las entidades CONTEXT, NETWORK, NETWORK-SERVICE y REFERENCE fueran borrados. Estos atributos fueron reemplazados con relaciones de las entidades anteriormente nombradas a la entidad SECURITY-CLASSIFICATION.

La mayor modificación del modelo fue la adición de una estructura completa para apoyar la posibilidad de almacenar como datos operacionales planes y ordenes de acuerdo a lo estipulado en las especificaciones del STANAG 2014 [34].

Esta nueva estructura está formada por las siguientes entidades; PLAN-ORDER, PLAN-ORDER-HEADER-CONTENT, PLANORDER- COMPONENT, PLAN-ORDER-COMPONENT-CONTENT, COMPONENT-HEADERCONTENT, COMPONENT-TEXT-CONTENT, PLAN-ORDER-COMPONENT-STRUCTURE, y PLAN-ORDER-COMPONENT-CONTENT-REFERENCE.

Otras entidades del modelo, como las estructuras de las entidades ACTION-TASK, AIRCRAFT-TYPE y CBRN-EVENT sufrieron la adición de nuevos requerimientos. También las entidades GEOGRAPHIC-FEATURE, GEOGRAPHIC-FEATURE-TYPE, MINEFIELD-MARITIME, NETWORK-SERVICE y VESSEL-TYPE sufrieron la adición de nuevos atributos.

### **2.7.3 Resumen de la comparación de las versiones del J3CIEDM**

Los principales cambios estructurales detectados en la evolución del J3CIEDM, desde su edición 3.0 publicada el 9 de diciembre del 2005, hasta su edición 3.1 publicada el 8 de diciembre del 2006, se pueden resumir de la siguiente forma:

La edición 3.1 cuenta con 30 entidades y 276 atributos más que la edición 3.0 del J3CIEDM. Estas 30 nuevas entidades son el fruto de los nuevos requerimientos operacionales surgidos durante 2005.

La edición 3.1 esta basada en 19 entidades independientes, mientras que la edición 3.0 esta basada en 15 entidades independientes.





### **SECCIÓN 3**

---



### **3 Diseño e implementación de modelos de datos y mecanismos de interoperabilidad aplicables a la gestión de emergencias civiles**

#### **3.1 Introducción**

En el presente capítulo se va a describir la principal aportación científica de la presente tesis doctoral. Basándonos en los resultados de la profunda investigación realizada en el capítulo anterior y en el conocimiento adquirido sobre el modelado de datos y más concretamente sobre los modelos de datos tácticos, se van a aplicar dichos conocimientos para implementar el esquema físico de dos de los modelos de datos tácticos más representativos, el C2IEDM versión 6.15c y el JC3IEDM Ed 3.0.

Una vez implementados los modelos de datos en un sistema gestor de bases de datos, se desarrollarán y compararán dos de las soluciones de interoperabilidad más extendidas actualmente, una basada en el estándar MIP y otra basada en el estándar NFFI. Con los resultados obtenidos en las pruebas de las aplicaciones de réplica, se propondrá un modelo de datos basado en la filosofía de núcleo común, para ser aplicado en la gestión de emergencias civiles.

El modelo de datos propuesto será integrado en el sistema de gestión de emergencias civiles SIMACOP y se validará en pruebas oficiales del programa CWID 2007, tanto nacionales como internacionales.

#### **3.2 Aplicación de los C2IS a la gestión conjunta de emergencias civiles**

Para el desarrollo del presente apartado se van a utilizar parte de los resultados de las investigaciones realizadas dentro de los siguientes proyectos de investigación nacionales e internacionales.

**TIN2004-03588**-C4ISR Multimedia aplicado a la gestión de emergencias [35]

**PASR-107900**-Mobile Autonomous Reactive Information system for Urgency Situations (MARIUS) [36]

**IST-34207**-DYnamic VIual NETwork (DYVINE) [37]

Una de las principales carencias detectadas en los análisis de la gestión de crisis graves en entornos civiles, es la falta de coordinación y de información entre los distintos mandos de los servicios de emergencias y de los distintos cuerpos y fuerzas de seguridad del estado, que participan en la resolución y/o mitigación de los efectos de una crisis.

La falta de una información actualizada entre agencias, que ofrezca un conocimiento de la situación global y una visión común del espacio de operaciones a los distintos mandos de las distintas agencias implicadas en la resolución de una crisis, sería la principal causa de la falta de coordinación entre los distintos cuerpos de seguridad o emergencias que colaboran sobre el terreno.

Esta falta de información se detecta tanto en el plano vertical, es decir, la adquisición y transmisión de información, hacia las autoridades al mando de la gestión de la crisis, por parte de las unidades desplegadas sobre el terreno, para que estas puedan coordinar esfuerzos y recursos de forma optima allí donde sean más necesarios, como en el plano horizontal, es decir, facilitar la capacidad de distribución de información actualizada entre las distintas unidades o nodos, de distintas agencias, que componen el operativo de actuación.

Para clarificar lo dicho anteriormente pasaremos a analizar el siguiente escenario ficticio de crisis civil;

El escenario propuesto se desarrolla en una gran ciudad con un importante puerto de mar, el inicio de la crisis sobreviene mientras se realizan las labores rutinarias de estiba de un carguero a primera hora de la mañana, en ese momento un contenedor de mercancías estalla con una fortísima explosión.

Una recreación de la crisis se puede ver en la figura 17, la onda expansiva de la explosión provoca daños y víctimas en un radio de 200 metros (Número (1) en figura 17), alcanza a los barcos atracados en las cercanías incendiándolos, se presume que al menos uno de ellos esta cargado con productos químicos (Número (2) en figura 17).

Además, alguno de los depósitos donde se almacena el carburante que los petroleros descargan se ha incendiado, pudiéndose incendiar los depósitos vecinos si dicho deposito estalla y provocar una reacción en cadena, que haría explotar todos esos enormes depósitos de combustible (Número (3) en figura 17).

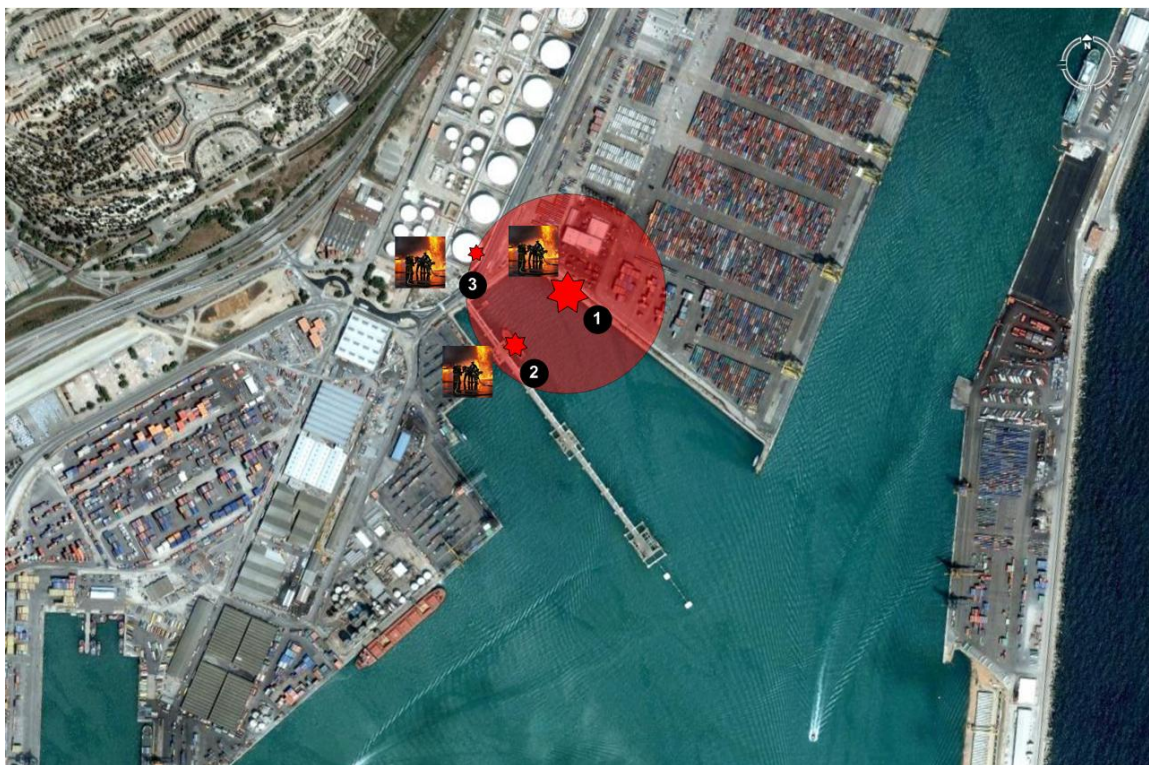


Figura 17

Las redes de telefonía móvil de la zona caen al destruirse alguna estación base de la zona y en las zonas adyacentes a la crisis quedan colapsadas por las llamadas y mensajes de los usuarios. La explosión se escucha en toda la ciudad provocando el pánico en la población, que colapsa los servicios de emergencias con llamadas, progresivamente se van colapsando las principales arterias de la ciudad que confluían en el puerto por un gran atasco.

Nada más conocerse el hecho, varias unidades pertenecientes a diversos cuerpos de seguridad (policía nacional, guardia civil y policía local) que se encontraban en las cercanías del puerto acuden a la zona de crisis, por otra parte bomberos y personal sanitario también llegan a las inmediaciones de la zona de crisis.

Todas estas unidades comienzan a realizar su trabajo, cada tipo de unidad trata de reportar información desde la zona de crisis a sus respectivos mandos utilizando principalmente la radio de sus respectivas unidades o en algunos casos la telefonía fija de las instalaciones del puerto, por lo tanto cada unidad describirá la parte de la crisis que ve desde su posición con lo que sus mandos directos contarán con un conocimiento de la situación parcial.

Las autoridades políticas reciben distintas versiones de la situación de los respectivos mandos de las unidades desplegadas, como hay riesgo de nubes químicas no se deja acceder a la prensa, con lo que no hay imágenes cercanas de la catástrofe, aunque no se evacua a la población civil cercana.

Con esta situación y en base a las distintas informaciones orales que llegan desde la zona, se toman las siguientes decisiones en los primeros momentos de la crisis;

- Como las autoridades sanitarias no conocen exactamente la extensión de la crisis ordenan montar rápidamente un hospital de campaña para atender a los heridos más urgentes, el cual queda situado a 200 metros de algunos de los depósitos de combustible más alejados de la crisis, que además están parcialmente ocultos por montones de contenedores. (Número (1) en figura 18).
- Los heridos evacuados, principalmente quemados, son dirigidos al hospital principal de la ciudad.

Transcurridos 45 minutos después de tomarse estas decisiones, ocurren los siguientes acontecimientos:

- Los bomberos, que no conocen la exacta localización del hospital de campaña, desisten de intentar apagar el depósito de combustible y se retiran, este depósito termina estallando y provocando una reacción en cadena en los depósitos cercanos que hace que el hospital de campaña sea alcanzado (Número (2) en figura 18).
- La unidad de quemados del principal hospital de la ciudad se colapsa y las rutas a los hospitales más cercanos están atascadas por vehículos.
- El barco que contenía productos químicos provoca una nube tóxica, que arrastrada por el viento, afecta a las viviendas situadas en un radio de 2 kilómetros de la zona de crisis (Número (3) en figura 18).

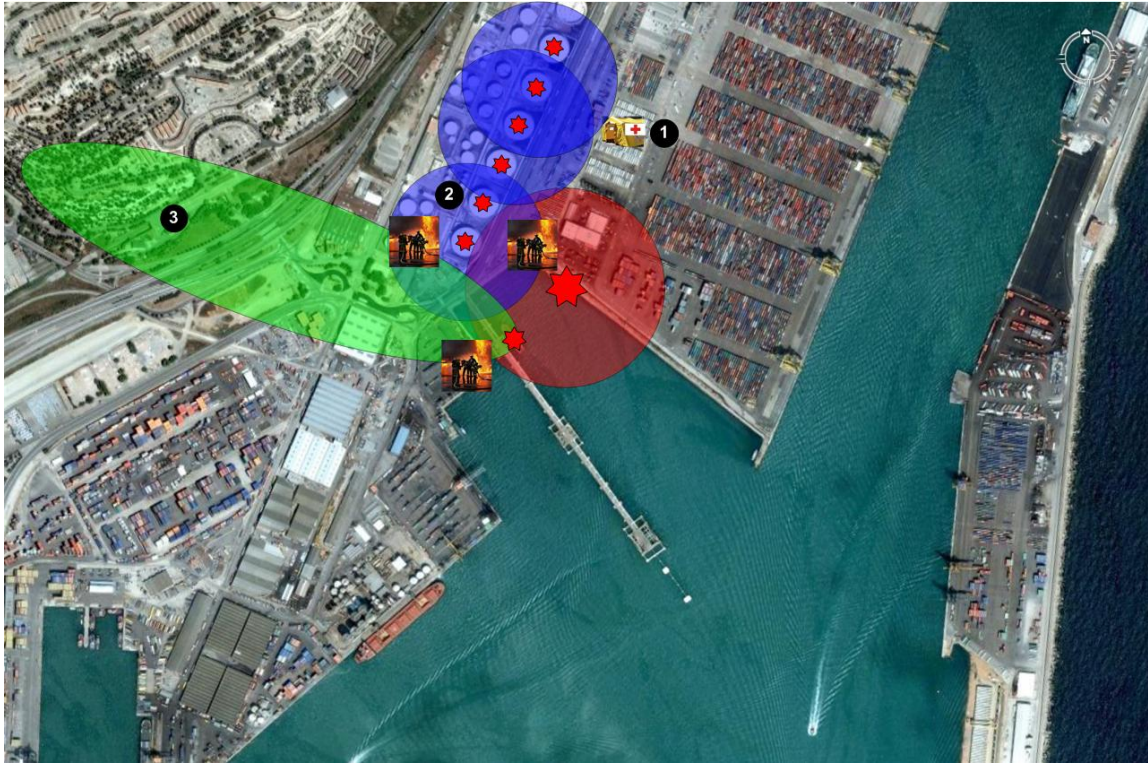


Figura 18

Este escenario, que puede parecer exagerado a primera vista, recoge faltas graves de coordinación entre mandos y entre las propias unidades sobre el terreno debidas a falta de información compartida, que pueden llegar a causar verdaderos desastres durante la resolución de una crisis.

Estas faltas de coordinación debidas a falta de información compartida se pueden detectar también en crisis civiles reales, un ejemplo lo podemos ver en el ataque terrorista a las torres gemelas el 11 de septiembre de 2001, donde la falta de información en tiempo real sobre la gravedad de los daños estructurales sufridos por los edificios tras los impactos de los aviones, hizo que las autoridades al mando de la gestión de la emergencia enviaran a más efectivos (bomberos principalmente) al interior de la torre sur minutos antes de que esta se colapsara [38].

Otro ejemplo que pone de manifiesto la falta de información sobre la situación del campo de operaciones permitió, que los primeros aviones con ayuda que llegaron a las zonas afectadas por el tsunami en 2004 llevaran principalmente mantas [39], siendo la temperatura de la zona en diciembre de unos 28 grados centígrados y la humedad superior al 80%, puesto que es temporada de lluvias en la región [40].

Queda pues de manifiesto, que ante crisis civiles de gran magnitud se hace necesario un conocimiento de la situación y una visión común del espacio de operaciones por parte de los mandos de las distintas fuerzas implicadas en la resolución de la crisis. Este conocimiento de la situación se obtendrá principalmente desde las unidades desplegadas sobre el terreno durante los primeros momentos de la crisis.

La información desde el espacio de operaciones, para ser realmente útil, debería ser compartida por todos los mandos al cargo de la resolución de la crisis en el nivel superior y a su vez, ser retransmitida, convenientemente procesada y actualizada, a las distintas unidades desplegadas sobre el terreno dependiendo de su posición en el espacio de operaciones, pudiendo de esta forma coordinar distintas unidades de distintos cuerpos de seguridad o emergencias, para optimizar su trabajo y evitar posibles peligros durante la resolución de la crisis.

Para que todo lo expuesto anteriormente fuera posible, haría falta un sistema distribuido de mando y control, que permitiera la localización de las unidades desplegadas, con un modelo de datos común, que además permitiera la interoperabilidad entre los distintos nodos del sistema mediante la réplica inmediata de los datos una vez introducidos en el sistema desde cualquier nodo del mismo.

Este sistema sería usado por todos los mandos responsables de la resolución de la crisis, teniendo todos, de esta forma, una idea común de la situación y un conocimiento detallado de la localización de todas las unidades sobre el terreno, así como imágenes en tiempo real de la zona del desastre.

Este sistema actualmente no existe en el ámbito civil, sólo los sistemas de mando y control militares dotados de modelos de datos tácticos con un núcleo común se asemejan al sistema descrito anteriormente.

Por lo tanto, en los siguientes apartados y como respuesta a algunos de los principales objetivos de la presente tesis doctoral, se van a describir diferentes métodos para implementar la interoperabilidad de los sistemas de mando y control y posteriormente se propondrán soluciones para adaptación de este tipo de sistemas de mando y control al ámbito civil y sobre todo para probar la viabilidad de la adaptación del concepto de un modelo de datos común a operaciones de gestión de crisis civiles.

Durante el desarrollo de la presente tesis se ha visto que las necesidades de la realidad de nuestro entorno confirman la utilidad de sistemas duales civiles y militares aplicables a la gestión de emergencias. La confirmación más evidente sería la creación de una unidad militar específica especializada en la gestión de emergencias civiles, la unidad militar de emergencia (UME).

La UME puede ser un laboratorio real perfecto para confirmar los planteamientos y conclusiones de la presente tesis.

### 3.3 Implementación del esquema físico del C2IEDM versión 6.15c

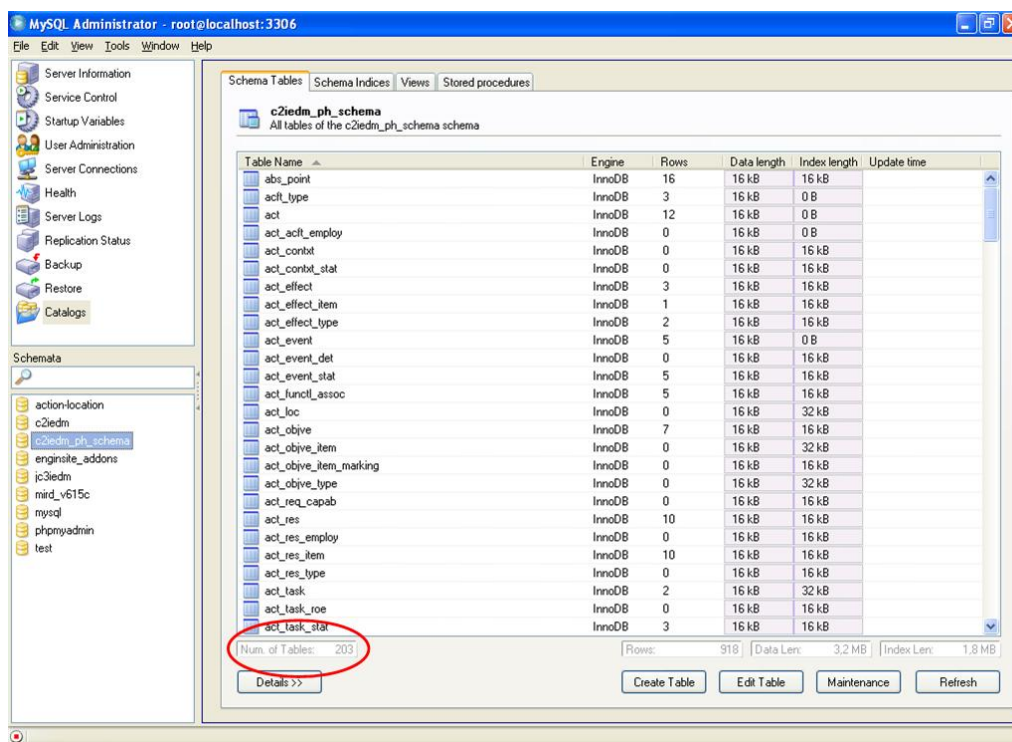
Para llevar a cabo la investigación en la que se basa la presente tesis doctoral, como base para la definición de un modelo de datos específico para la gestión de emergencias, no solo se requería un conocimiento minucioso de los diferentes modelos de datos tácticos y de sus diferentes versiones, era necesaria la implementación de los esquemas físicos de algunos de los modelos de datos analizados para realizar diversas de las pruebas de interoperabilidad entre sistemas de mando y control, que nos ayudarán a formular las conclusiones de esta tesis doctoral.

El primero de los modelos de datos tácticos implementados en la presente tesis fue el C2IEDM versión 6.15c. Se escogió esta versión del modelo de datos porque era la versión central de las cinco versiones del modelo y era la que minimizaba las diferencias entre todas las demás versiones del modelo que fueron publicadas entre los años 2004 y 2005.

El objetivo de este apartado es mostrar las categorías de información cubiertas por el modelo de datos que son de interés para los usuarios operacionales del modelo.

En primer lugar se mostrarán las 203 tablas de la base de datos implementada, junto con todas sus relaciones, las cuales representan a las 203 entidades con sus 1433 atributos que componen el C2IEDM v6.15c.

En la figura 19 se pueden ver las 203 tablas que componen la base de datos que implementa el esquema físico del C2IEDM v6.15c. Como gestor de bases de datos se ha utilizado el programa MySQL Administrator versión 4.1.12 [41].



The screenshot shows the MySQL Administrator interface for the 'c2iedm\_ph\_schema' database. The main window displays a list of tables with columns for Table Name, Engine, Rows, Data length, Index length, and Update time. The 'Num of Tables' field at the bottom left is circled in red and shows the value 203. The 'Rows' field shows 919, 'Data Len' shows 3.2 MB, and 'Index Len' shows 1.8 MB. There are buttons for 'Create Table', 'Edit Table', 'Maintenance', and 'Refresh' at the bottom right.

Table Name	Engine	Rows	Data length	Index length	Update time
abs_point	InnoDB	16	16 kB	16 kB	
act_type	InnoDB	3	16 kB	0 B	
act	InnoDB	12	16 kB	0 B	
act_act_employ	InnoDB	0	16 kB	0 B	
act_conbit	InnoDB	0	16 kB	16 kB	
act_conbit_stat	InnoDB	0	16 kB	16 kB	
act_effect	InnoDB	3	16 kB	16 kB	
act_effect_item	InnoDB	1	16 kB	16 kB	
act_effect_type	InnoDB	2	16 kB	16 kB	
act_event	InnoDB	5	16 kB	0 B	
act_event_det	InnoDB	0	16 kB	16 kB	
act_event_stat	InnoDB	5	16 kB	16 kB	
act_funcnt_assoc	InnoDB	5	16 kB	16 kB	
act_loc	InnoDB	0	16 kB	32 kB	
act_objive	InnoDB	7	16 kB	16 kB	
act_objive_item	InnoDB	0	16 kB	32 kB	
act_objive_item_marking	InnoDB	0	16 kB	16 kB	
act_objive_type	InnoDB	0	16 kB	32 kB	
act_req_capab	InnoDB	0	16 kB	16 kB	
act_res	InnoDB	10	16 kB	16 kB	
act_res_employ	InnoDB	0	16 kB	16 kB	
act_res_item	InnoDB	10	16 kB	16 kB	
act_res_type	InnoDB	0	16 kB	16 kB	
act_task	InnoDB	2	16 kB	32 kB	
act_task_roe	InnoDB	0	16 kB	16 kB	
act_task_stat	InnoDB	3	16 kB	16 kB	

Figura 19



En la figura 20 se pueden ver los 315 índices que componen todas las relaciones entre las distintas entidades del modelo.

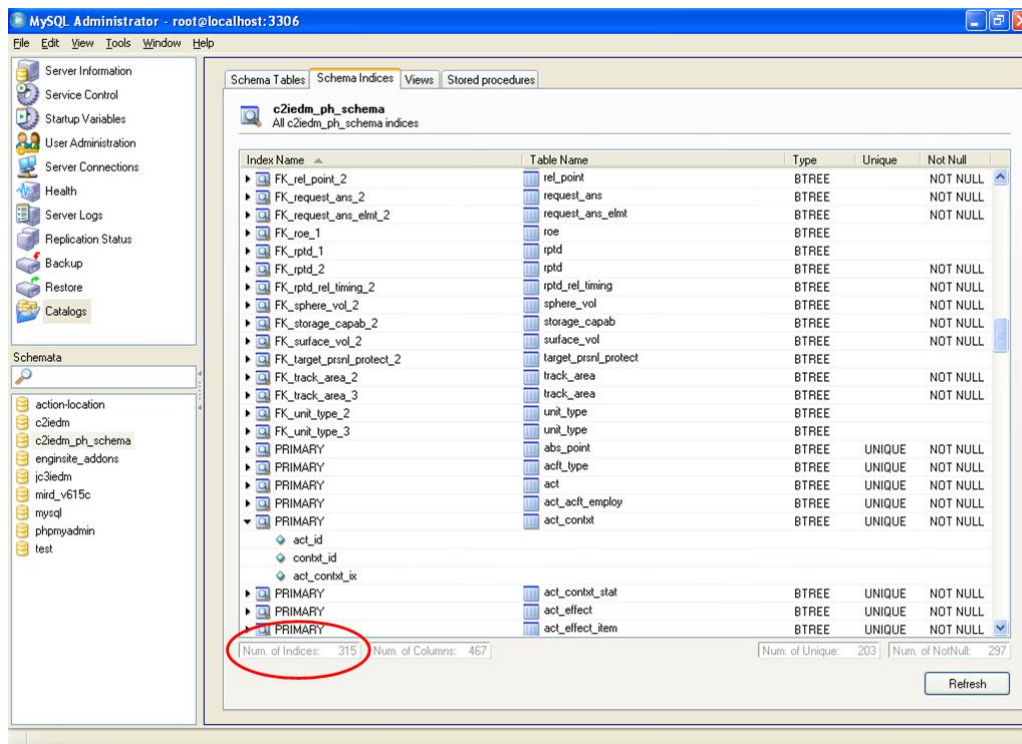


Figura 20

No existe un camino lineal que pueda ser seguido de forma lógica, a través de todas sus entidades, para revisar un modelo de datos táctico como el C2IEDM v6.15c. El gran número de relaciones que existen entre las distintas entidades del esquema relacional hace que casi cada parte del modelo dependa de otras partes del mismo, por este motivo, en el presente apartado se va a organizar la estructura del modelo de datos de una forma que sea lo más descriptiva y clara posible para el lector.

Con este fin, se va a dividir la estructura lógica del modelo en cuatro partes claramente diferenciadas:

1. Objetos de interés y sus propiedades inherentes
2. Situaciones pasadas, presentes o futuras representadas por actos sobre los objetos
3. Actividades pasadas, presentes o futuras en las que los objetos están involucrados
4. Mecanismos para agrupar datos en paquetes de información.

Dentro de estas cuatro partes se van a describir, a nivel de entidad, las principales entidades que componen el modelo así como sus relaciones con otras entidades dependientes de las mismas.

### 3.3.1 Objetos de interés

Una tarea básica en especificación de datos es la definición del universo del discurso, como primera tarea se seleccionan los objetos sobre los cuales se va a almacenar información, en el caso del C2IEDM estos objetos son los siguientes: Materiales, Infraestructuras, Organizaciones, Características y Personas.

Dentro del diseño del modelo se diferencian dos grandes tipos de objetos:

- **Items:** Aquellos que pueden ser identificados individualmente (por su nombre; Sargento Juan Garcia, 7ª brigada aerotransportada, por su número de serie, placa de autorización, etc.)
- **Types:** Aquellos que presentan propiedades de grupos o clases (un carro de combate, un barco, un helicóptero, un soldado de infantería, un refugiado, etc.)

Las dos categorías son utilizadas en paralelo como elementos estructurales básicos del modelo de datos y ambas están relacionadas la una con la otra. Las características de los datos son introducidas en el sistema o bien en la parte de los ítems individuales o bien en la parte de los tipos según convenga.

Algunas características descritas en la parte de tipos también son aplicadas al ítem cuando un ítem es asignado a un tipo de clasificación. El enlace entre ítem y tipo es obligatorio en el modelo de datos.

La estructura del C2IEDM etiqueta objetos de clase como OBJECT-TYPE e identifica individualmente instancias como OBJECT-ITEM. En esta distinción entre tipos e ítems individuales esta implícito que los datos relativos a OBJECT-TYPES tenderán a ser relativamente estáticos o permanentes en el tiempo, o lo que es lo mismo que los valores de los atributos no cambian muy a menudo, mientras que los datos relativos a OBJECT-ITEMs serán probablemente más dinámicos.

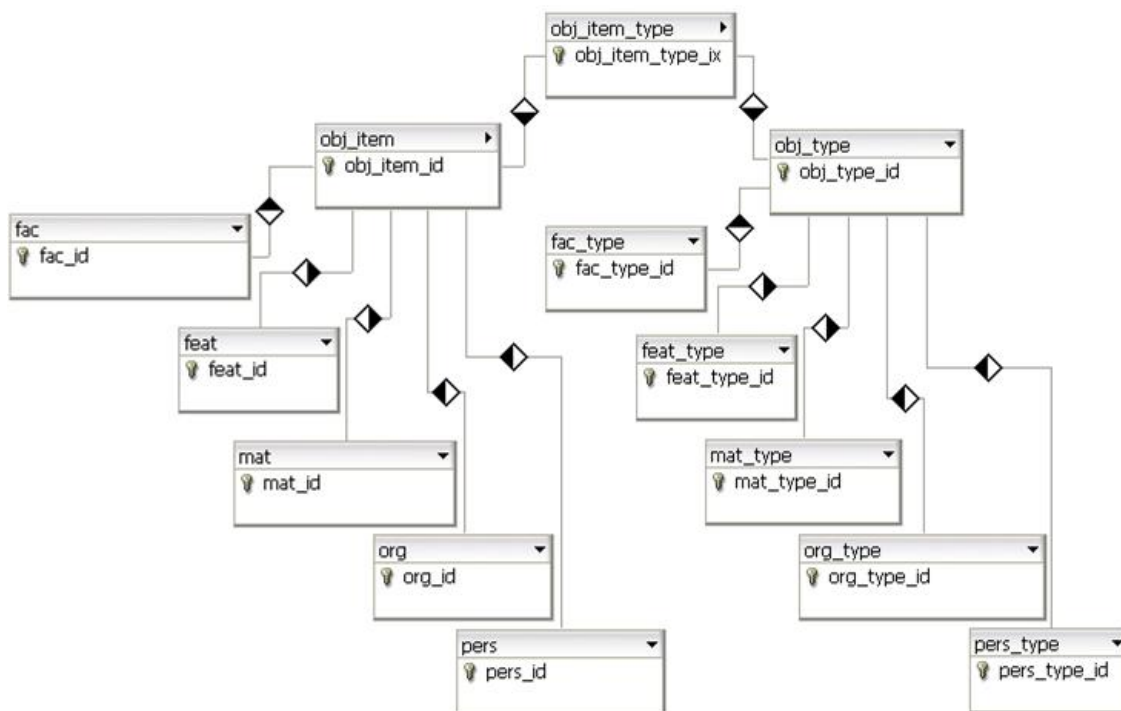
Por ejemplo, si una característica es de un tipo (M1A1 Abrams Tank), entonces es un atributo OBJECT-TYPE, de esta forma el calibre del cañón principal, la anchura del vehículo, el tipo de blindaje son características OBJECT-TYPE.

Sin embargo, el nivel de combustible, la cantidad de munición que tiene, el actual estado operacional de un carro de combate con un número de serie concreto son características de un OBJECT-ITEM. Por lo tanto, la obligatoriedad de clasificar una instancia de OBJECT-ITEM como una instancia de OBJECT-TYPE asegura que el ítem hereda todas las características del tipo.

Hay cinco categorías de subtipos que abarcan cualquier objeto incluido en el modelo de datos: FACILITY, FEATURE, MATERIEL, ORGANISATION y PERSON.

Un subtipo es la misma cosa que su “padre”, pero él tiene algunas propiedades que no son aplicables a sus “hermanos”.

Los objetos ítem y tipo están divididos en una extensa jerarquía. Los primeros niveles de esta jerarquía son paralelos y se muestran en la figura 21.



**Figura 21**

Las relaciones de “muchos a muchos” entre objetos OBJECT-TYPE y OBJECT-ITEM se resuelven a través de una entidad asociativa llamada OBJECT-ITEM-TYPE, como se puede ver en la parte superior de la figura 21.

Las instancias de esta entidad se definen como la clasificación percibida de un objeto OBJECT-ITEM como un objeto OBJECT-TYPE concreto.

La presencia del atributo “object-item-type-index” permite el realizar distintas clasificaciones de un objeto a lo largo de un periodo de tiempo. Por ejemplo un objeto OBJECT\_ITEM (item id 911), podría ser clasificado en un primer reporte como un objeto OBJECT-TYPE desconocido (type id 10741), en un segundo reporte como un objeto OBJECT-TYPE vehiculo (type id 10741) y finalmente en un último reporte como un objeto OBJECT-TYPE carro de combate T72 (type id 133794).

Las definiciones de las entidades subtipo tanto de objetos ítem como de objetos tipo se muestran en la Tabla 8, como se podía esperar los dos conjuntos de definiciones a este nivel son muy similares.

<b>Entidad</b>	<b>Definición de la entidad</b>
FACILITY	Un OBJECT-ITEM que es construido, instalado o establecido para algún propósito particular y identificado por el servicio de aporta en vez de por su contenido.
FACILITY-TYPE	Un OBJECT-TYPE que es construido, instalado o establecido para algún propósito particular y identificado por el servicio de aporta en vez de por su contenido. Ejemplos serían; un puesto de reabastecimiento de combustible, un hospital.

FEATURE	Un OBJECT-ITEM que abarca características metereológicas, geográficas y de control que tienen alguna importancia militar.
FEATURE-TYPE	Un OBJECT-TYPE que abarca características metereológicas, geográficas y de control que tienen alguna importancia militar. Ejemplos serían; un bosque, un área de lluvia, un río, un área de responsabilidad.
MATERIEL	Un OBJECT-ITEM que es equipamiento, aparato o suministro sin distinción en cuanto a su aplicación ya sea con propósito administrativo o de combate.
MATERIEL-TYPE	Un OBJECT-TYPE que es equipamiento, aparato o suministro sin distinción en cuanto a su aplicación ya sea con propósito administrativo o de combate. Ejemplos serían; barcos, tanques, aviones, etc. Se incluyen también los repuestos, equipamiento de apoyo pero, se excluyen instalaciones y servicios.
ORGANISATION	Un OBJECT-ITEM que es una estructura administrativa y funcional.
ORGANISATION-TYPE	Un OBJECT-TYPE que representa estructuras administrativas y funcionales.
PERSON	Un OBJECT-ITEM que es un ser humano con una importancia militar reconocida.
PERSON-TYPE	Un OBJECT-TYPE que representa un ser humano cuya información debe ser almacenada.

**Tabla 8. Entidades subtipo de primer nivel tanto de objetos ítem como de objetos tipo**

En la figura 22 se puede ver desarrollada toda la estructura de la entidad OBJECT-ITEM, en esta figura se pueden ver además de los 5 subtipos de primer orden en los que se descompone la entidad OBJECT-ITEM y que se mostraban en la figura 21 de la presente tesis doctoral, todos los subtipos de segundo orden que componen cada uno de estos subtipos de primer orden con sus correspondientes subdivisiones.

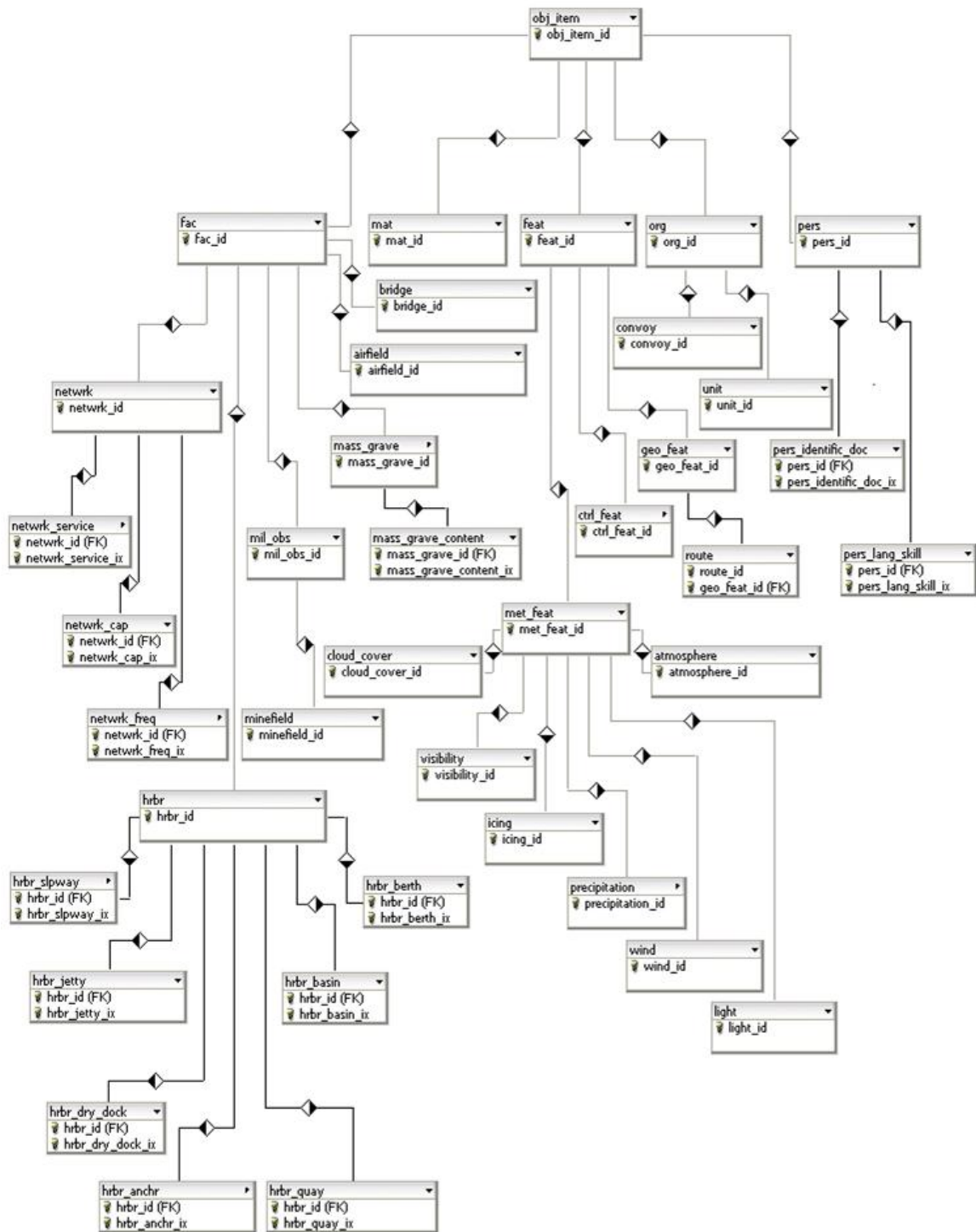


Figura 22

En la figura 23 se puede ver desarrollada toda la estructura de la entidad OBJECT-TYPE, en esta figura se pueden ver además de los 5 subtipos de primer orden en los que se descompone la entidad OBJECT-TYPE y que se mostraban en la figura 21 de la presente tesis doctoral, todos los subtipos de segundo orden que componen cada uno de estos subtipos de primer orden con sus correspondientes subdivisiones.

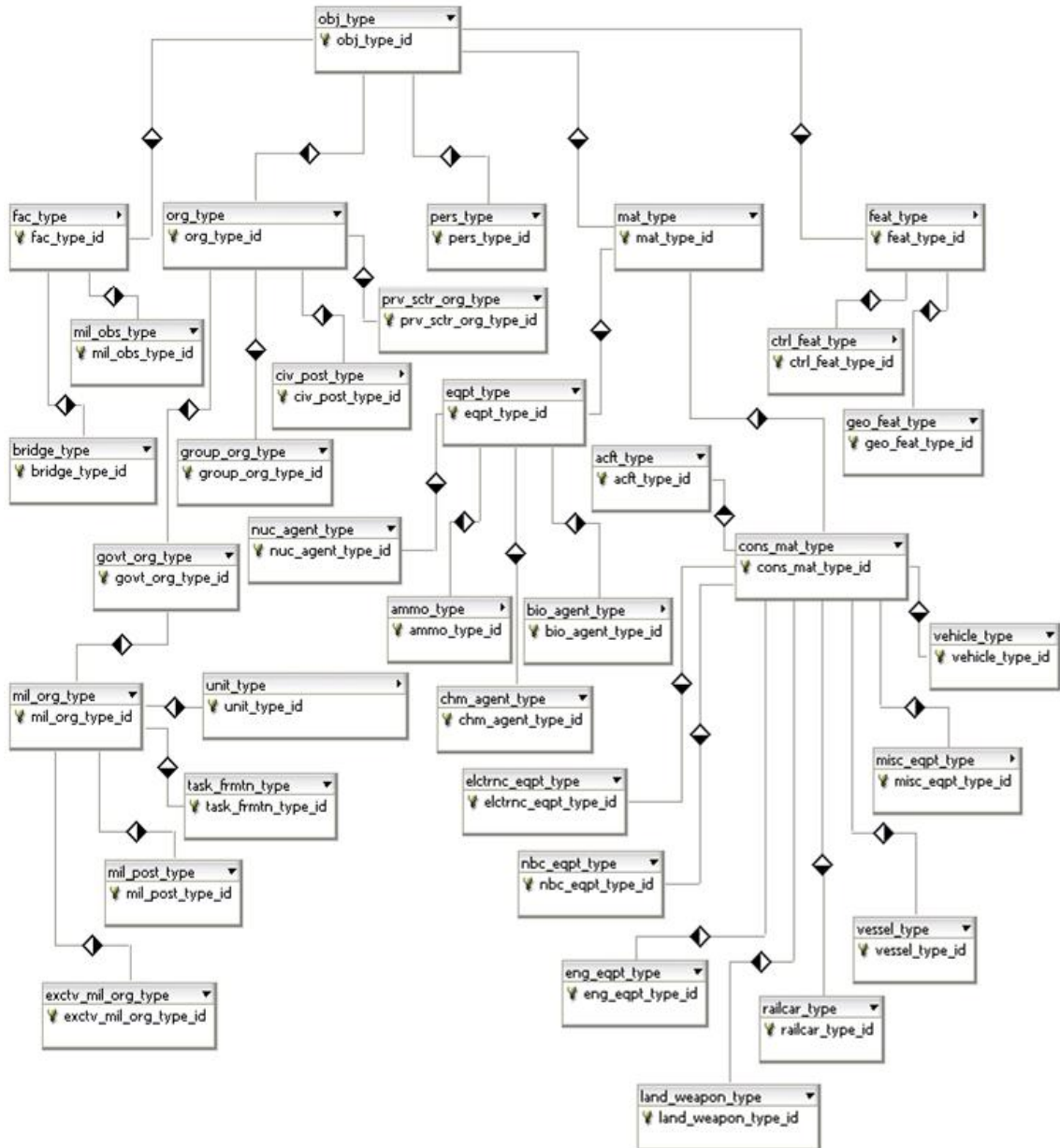


Figura 23

### 3.3.2 Situación

Con la palabra situación se abarca un amplio conjunto de informaciones relativas a los objetos que se almacenan en distintas estructuras de datos dentro del modelo de datos, estas informaciones incluyen relaciones “tipo con tipo” (type-to-type), relaciones “ítem con tipo” (item to type), capacidades de ítems o tipos, afiliaciones de ítems o tipos, estado de ítems, localización de ítems y relaciones ítem con ítem (item to item). En esta apartado se van a describir y a mostrar alguna de estas estructuras de datos relacionadas con la situación de los objetos, estas estructuras de datos han sido extraídas de la implementación del esquema físico del C2IEDM v6.15c que se ha realizado como parte de la investigación que se ha llevado a cabo en la presente tesis doctoral.

La primera de las estructuras de datos que se van a describir sería la encargada de almacenar información relativa al estado de los objetos.

La entidad en la que se basa la percepción del estado de los objetos ítem sería la entidad OBJECT-ITEM-STATUS y su estructura se puede ver en la figura 24. Los subtipos de dependientes de esta entidad contienen atributos que describen el estado de los objetos, por ejemplo el estado de una unidad enemiga podría almacenarse en un rango de estados desde “Totalmente operativo” a “Destruído”, o por ejemplo el estado de un soldado podría ser “listo”, “incapacitado”, “arrestado”, “capturado”, etc. Una de las entidades subtipo de OBJECT-ITEM-STATUS es MEDICAL-FACILITY-STATUS cuya estructura no se muestra en la figura 21. Esta entidad y su estructura permiten almacenar un gran número de detalles relacionados con los tipos de pacientes que tiene un hospital militar, sus llegadas, cirugías previstas, defunciones, etc.

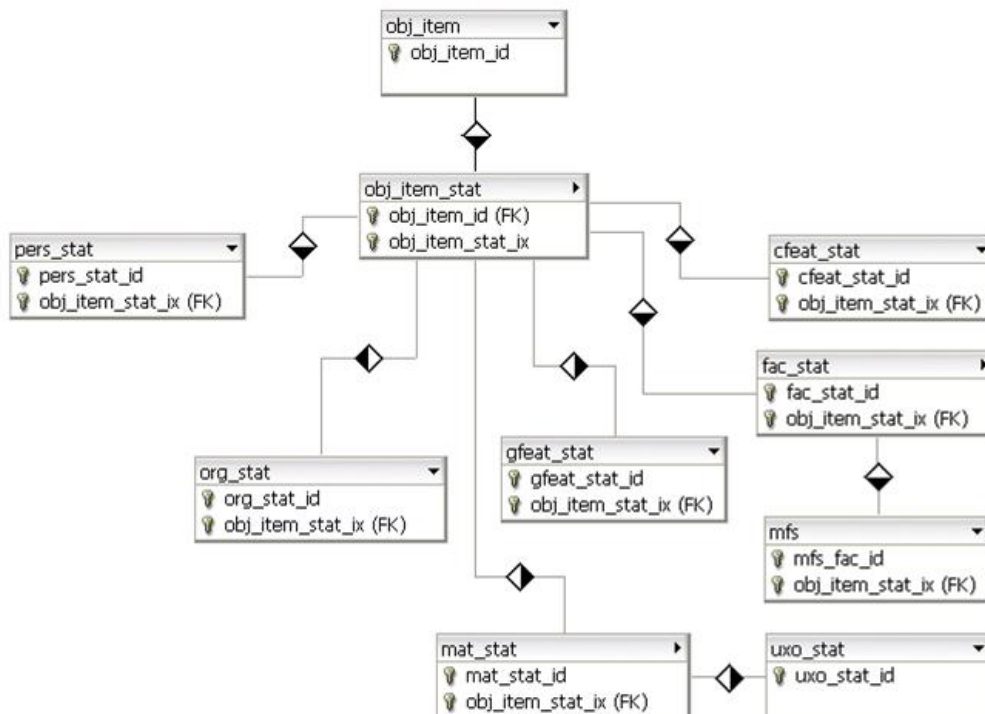


Figura 24

Todas estas estructuras de datos permiten acceder a múltiples registros sobre el estado de una instancia de la entidad OBJECT-ITEM y de esta forma reflejar la evolución del estado de los objetos en un periodo de tiempo determinado. Estos registros proporcionan informaciones útiles tanto como para saber el estado de un simple soldado como para planificar que fuerzas y recursos son necesarios en una operación basándose en el registro del estado de las unidades enemigas.

Las siguientes estructuras de datos relativas a la situación de los objetos que se van a describir son las que especifican el acceso y la localización de los objetos.

La entidad independiente ADDRESS y su estructura de datos dependiente especifican un acceso del tipo “dirección” para cada objeto. El modelo de datos permite múltiples formas de contacto o dirección para los objetos, desde una dirección de correo electrónico o un número de teléfono para las personas a una dirección postal para un edificio.

La entidad ADDRESS tiene dos subtipos PHYSICAL-ADDRESS y ELECTRONIC-ADDRESS, esta estructura permite asociar cualquier número de accesos distintos a una instancia OBJECT-ITEM a través de la entidad OBJECT-ITEM-ADDRESS. La estructura completa de la entidad ADDRESS se puede ver en la figura 25.

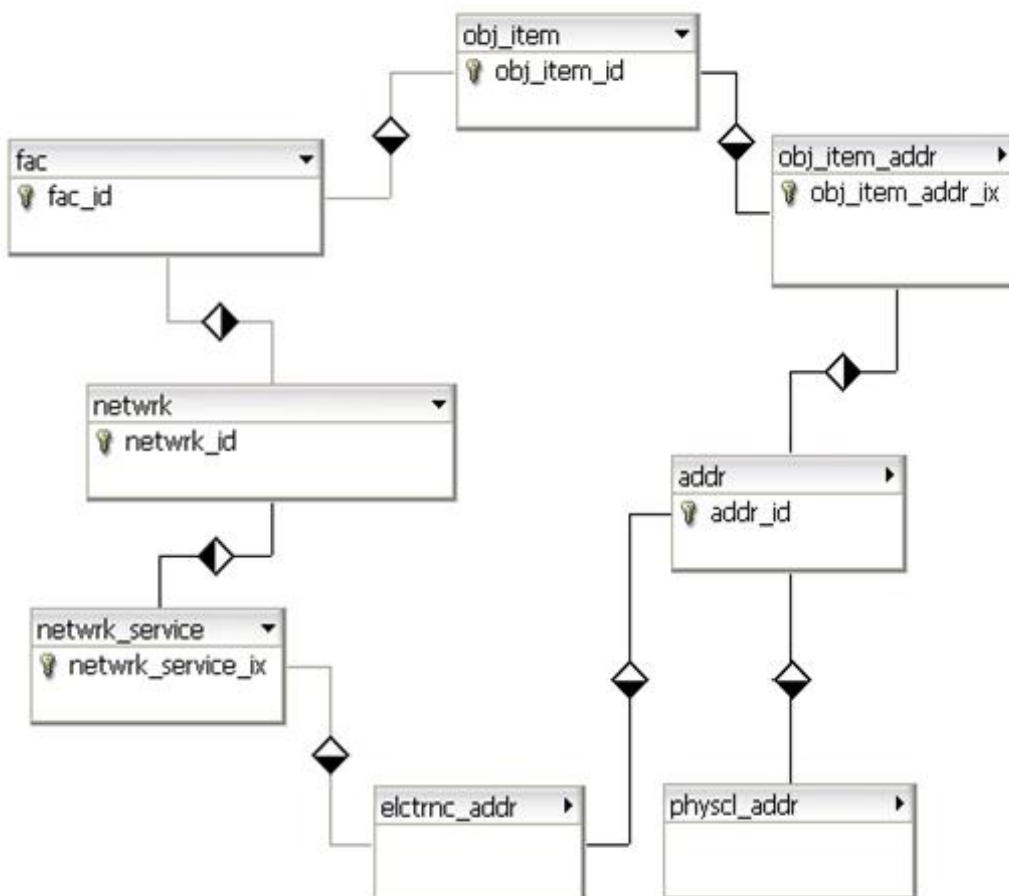


Figura 25



La entidad independiente LOCATION agrupa, dentro del modelo de datos, dos conceptos muy relacionados entre sí y de gran interés para los planificadores de operaciones. Estos conceptos son los siguientes:

- La especificación de la geometría requerida para describir objetos.
- El emplazamiento de objetos o de su geometría asociada tanto con respecto a la superficie de la tierra como con respecto a otros objetos.

La posibilidad de poder especificar geometrías permite la descripción de varios tipos de fronteras o regiones como pueden ser corredores, orbitas, líneas, regiones, etc. Todos estos objetos geométricos son empleados en la planificación de operaciones.

Junto a este tipo de objetos el C2IEDM v6.15c permite el posicionamiento de objetos con respecto a la superficie de la tierra o respecto a otros objetos. Este posicionamiento de objetos se realiza mediante la relación entre las entidades OBJECT-ITEM y LOCATION, esta relación se realiza a través de la entidad OBJECT-ITEM-LOCATION.

El elemento básico utilizado tanto en la localización de objetos como en la generación de objetos geométricos es el “punto” a partir de él se generan el resto de estructuras geométricas. Una línea está compuesta por puntos, una línea poligonal está compuesta por varias líneas, una región está delimitada por una línea poligonal que termina cerrándose, es decir, que el primer punto de la línea y el último coinciden, una elipse queda completamente definida por tres puntos, etc.

En cuanto a la localización de un punto esta puede hacerse de forma absoluta o relativa, es decir se localiza a un objeto sobre la superficie de la tierra o se le localiza con respecto a otros objetos de posición conocida. La distancia vertical del punto se puede medir de varias maneras a través de la entidad VERTICAL-DISTANCE, ya sea con respecto al nivel del mar o con respecto a la superficie del terreno en ese punto.

La posibilidad de poder contar con distancias verticales de puntos da la oportunidad de generar volúmenes a través de regiones y puntos elevado, ejemplos de volúmenes que se pueden generar dentro del modelo pueden ser conos, cilindros, cubos, casquetes esféricos, semiesferas, etc.

La vista completa de la estructura asociada a la entidad LOCATION se puede ver en la figura 26.

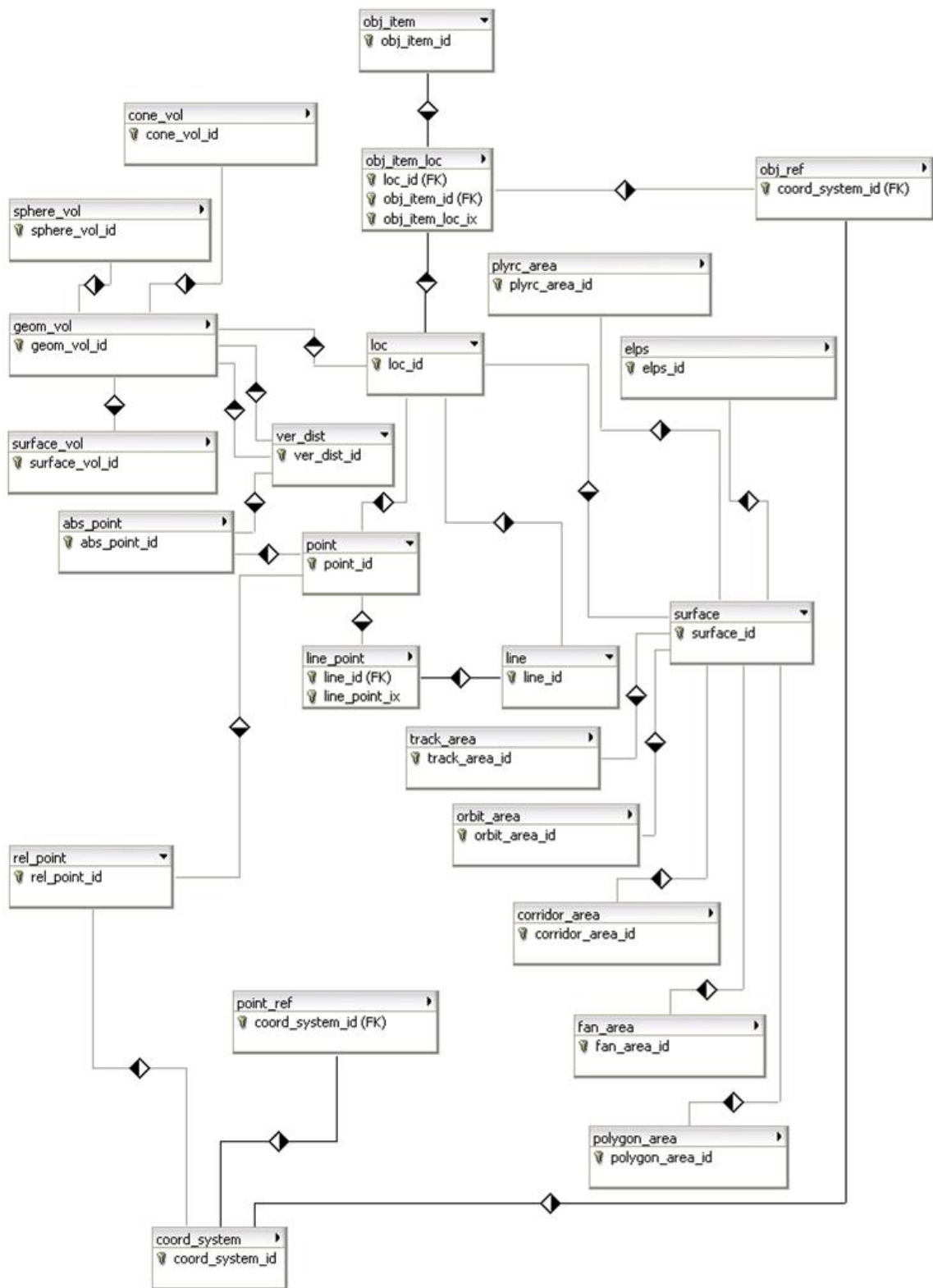


Figura 26

La última estructura de datos relativa a la situación de los objetos que se va a describir en este apartado es la que especifica las capacidades de los objetos tanto ítems como tipos.

La especificación y monitorización de las capacidades de los objetos es un factor importante dentro del proceso de planificación militar. El poder conocer la capacidad de los objetos puede ayudar en el análisis de viabilidad de las acciones en las que están involucradas fuerzas aliadas o en la evaluación de probabilidad de éxito de las operaciones en las que están envueltas fuerzas enemigas.

Las instancias relativas a capacidad pueden estar sujetas a varios tipos de condiciones, por ejemplo, la velocidad con la que puede maniobrar un vehículo dependerá del tipo de terreno sobre el que se encuentre dicho vehículo o el alcance de un arma puede depender del tipo de munición con la que se la cargue.

Por lo tanto la estructura de la entidad CAPACITY está diseñada para abarcar dos conceptos: La necesidad de caracterizar la capacidad de un objeto y a su vez enlazar estas capacidades con otras partes del modelo de datos donde se usan especificaciones de capacidad.

Podemos definir capacidad como la potencial habilidad de realizar algún trabajo, llevar a cabo alguna acción o misión, alcanzar algún objetivo o facilitar algún servicio.

La entidad CAPACITY representa la lista genérica de capacidades que se pueden aplicar a objetos o a sus tipos. Esta lista cubre un amplio rango de habilidades como su velocidad máxima o su máxima capacidad de almacenaje, algunas de estas capacidades no son aplicables a ciertas clases de objetos o clases.

La lista de habilidades se almacena en los atributos “capability-category-code” y “capability-subcategory-code”, el primer atributo se refiere a clases generales de habilidades, por ejemplo, la habilidad de transportar cosas, mientras que el segundo atributo se refiere a las habilidades específicas de una clase, por ejemplo, la habilidad de transportar un determinada cantidad de líquido. Los subtipos de la entidad CAPABILITY añaden información adicional para ciertas clases de capacidades.

La entidad CAPABILITY está relacionada con tres entidades independientes con el fin de facilitar las siguientes funciones:

- Especificar la capacidad normal o esperada para un objeto OBJECT-TYPE: El valor estándar de la capacidad de un objeto OBJECT-TYPE se define a través de la entidad OBJECT-TYPE-CAPABILITY-NORM.
- Estimar la capacidad actual de un objeto OBJECT-ITEM: La capacidad de objetos OBJECT-ITEM individuales puede variar por causa de varios factores, la entidad OBJECT-ITEM-CAPABILITY almacena el valor percibido de la capacidad de un objeto OBJECT-ITEM.

La vista completa de la estructura asociada a la entidad CAPABILITY se puede ver en la figura 27

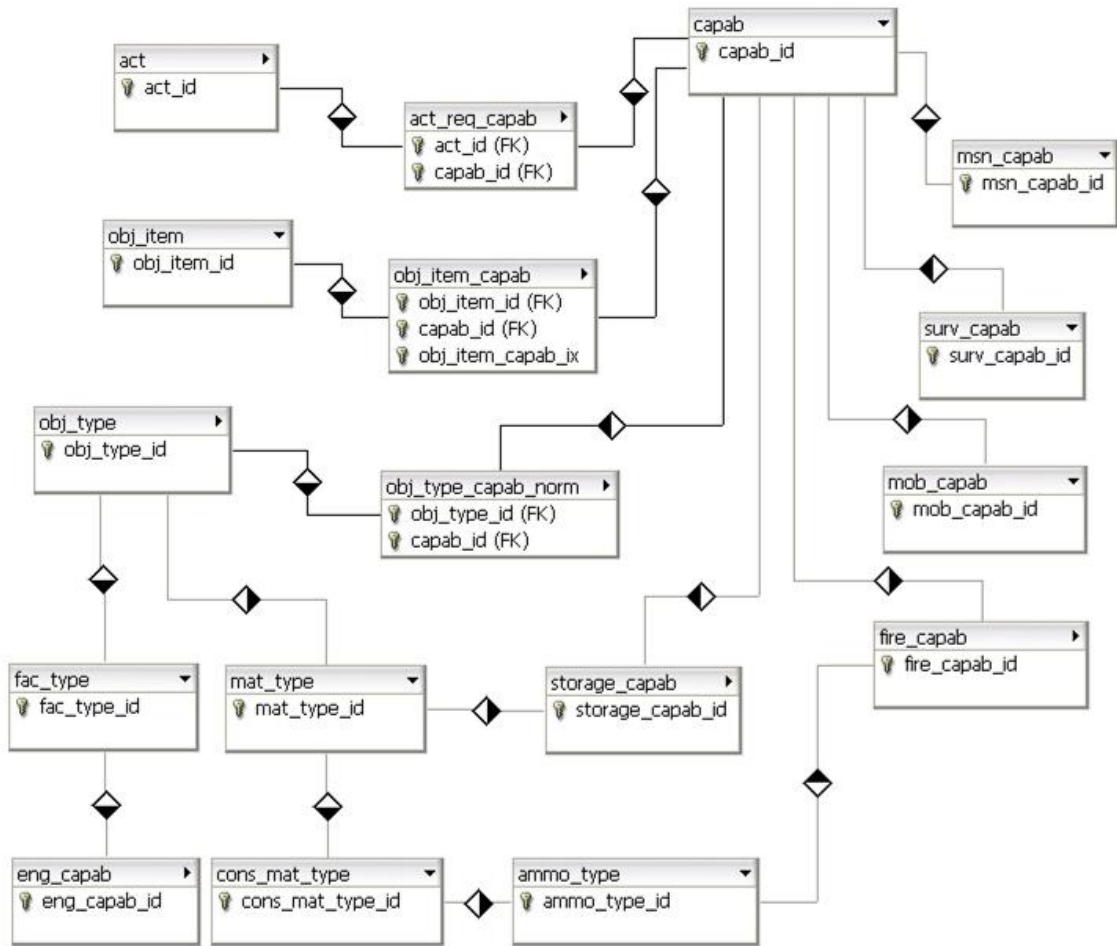


Figura 27

### 3.3.3 Actividad

El termino actividad hace referencia a reporte de eventos y planificación de acciones. Los planes de las acciones que se van a llevar a cabo deben ser transformados en órdenes, el modelo de datos debe responder a esta necesidad ya que toda planificación de una acción afecta al uso de objetos, recursos, objetivos o efectos de actividad. En este apartado vamos a describir los conceptos básicos del C2IEDM para representar actividad.

La entidad independiente ACTION es la base de esta representación dentro del modelo. Su estructura asociada incluye mecanismos para especificar objetos, ítem o tipo, como recursos y objetivos cuyo uso o consecución implica actividad, almacenar efectos de actividades, clasificar actividades, mantener un histórico del estado de las actividades y relacionar actividades con otras partes del modelo, como localizaciones o capacidades para llevar a cabo una acción.

La base conceptual para modelar acciones está basada en una declaración en la cual “algo” lleva a cabo una actividad que afecta a “algo o a alguien” en un tiempo determinado. Dentro el modelo ese “algo” mencionado en la declaración básica de actividad es representado bien por un objeto OBJECT-TYPE o bien por un objeto OBJECT-ÍTEM, de esta forma objetos ítem y tipo se relacionan con acciones de dos formas distintas; como recursos o como objetivos.

Las entidades ACTION-RESOURCE y ACTION-OBJECTIVE han sido introducidas para poder asignar roles a objetos OBJECT-TYPE u objetos OBJECT-ÍTEM como partes de la especificación de una acción.

ACTION-RESOURCE se define como un objeto OBJECT-TYPE o un objeto OBJECT-ÍTEM que es requerido, posicionado o usado de cualquier otra forma en el desarrollo de una acción específica.

ACTION-OBJECTIVE se define como el objeto OBJECT-TYPE o el objeto OBJECT-ÍTEM que se convierta en el objetivo de la especificación de una acción.

Como un ejemplo del uso de los objetos ACTION-RESOURCE y ACTION-OBJECTIVE como recursos y objetivos podríamos describir la siguiente acción: La brigada número 11 del ejército holandés puede usar 4 helicópteros Chinook (objetos tipo usados como objetos ACTION RESOURCE) para transportar 100 unidades de tropa a la zona de aterrizaje Alpha (objetos tipo usados como objetos ACTION OBJECTIVE).

Existe una tercera relación entre objetos operacionales y la entidad ACTION, esta tercera relación es la que caracteriza los efectos de una acción. La efectividad y los efectos de las acciones dentro del espacio de operaciones deben ser monitorizadas para ayudar a estimar la efectividad de dichas acciones, para esta contingencia se ha definido la entidad ACTION-EFFECT como la efectividad percibida de una determinada acción llevada a cabo contra un determinado objetivo, que puede ser tanto un objeto OBJECT-ITEM como un objeto OBJECT-TYPE.

Un ejemplo del uso de la entidad ACTION-EFFECT sería el siguiente reporte: tras una determinada acción las fuerzas enemigas se han reducido en un 50% y la posición ha sido tomada.

El objeto ACTION-EFFECT estimado especifica una cantidad si el objetivo es un objeto OBJECT-TYPE o una fracción si el objetivo es un objeto OBJECT-ITEM. Las operaciones llevadas a cabo se evalúan comparando los objetos ACTION-EFFECT generados con los objetos ACTION-OBJECTIVE declarados previamente.

Otra característica importante de los objetos ACTION-EFFECT es que pueden capturar información sobre efectos de una acción sobre objetos que no estaban entre los objetivos iniciales de dicha acción, a esta información se la conoce como daños colaterales.

La vista completa de la estructura asociada a la entidad CAPABILITY se puede ver en la figura 28.

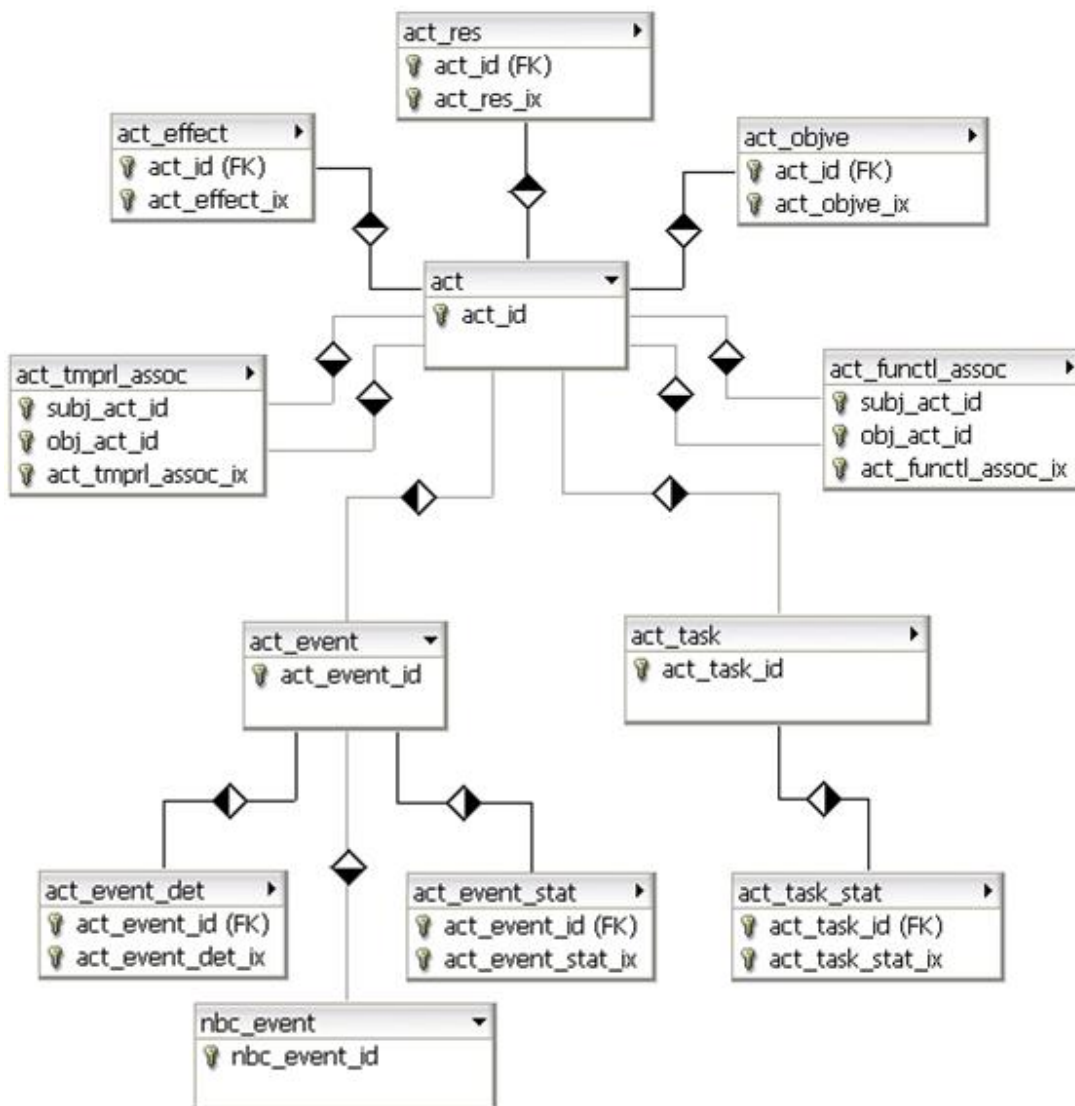


Figura 28

La ejecución de una determinada acción depende de una compleja asociación de tareas y órdenes. Estas tareas y órdenes deben tener una estricta sincronización temporal de forma que por ejemplo se ha de indicar de alguna manera que la acción B no puede empezar a ejecutarse hasta que la acción A haya concluido.

A tal efecto el C2IEDM incluye dos entidades asociativas que especifican la dependencia entre acciones y permite la creación de jerarquías, esta dos entidades se pueden ver en la figura 25 y son las siguientes:

- ACTION-FUNCTIONAL-ASSOCIATION especifica relaciones funcionales entre acciones.
- ACTION-TEMPORAL-ASSOCIATION especifica dependencias temporales entre acciones.

Los subtipos de la entidad independiente ACTION son las entidades ACTION-EVENT y ACTION-TASK, y son usadas para describir distintos tipos de actividades que implican diferentes requerimientos, por otro lado las entidades encargadas de almacenar el estado de las acciones son ACTION-EVENT-STATUS y ACTION-TASK-STATUS, todas estas entidades se pueden ver también en la figura 28.

### 3.3.4 Agrupación de datos

El modelo C2IEDM contiene una estructura de agrupación de información cuya base es la entidad independiente REPORTING-DATA, esta estructura está relacionada con muchas de las entidades que representan datos dinámicos dentro del modelo.

Una considerable cantidad de información sobre la situación del campo de operaciones consiste en reportes realizados por personas u organizaciones. Estos reportes generalmente contienen información sobre datos dinámicos, como localizaciones, estados o composición de agrupaciones de tropas, además se debe incluir en la clasificación de los reportes si estos se refieren a elementos amigos, hostiles o neutrales.

Por otro lado hemos de tener en cuenta la fiabilidad de la fuente de la información, la fecha y la hora del reporte o su validez temporal. El modelo captura todo este tipo de información a través de la entidad REPORTING-DATA y sus subtipos.

La recolección de toda esta información, amplificada por las diferentes fuentes desde la que pueden llegar reportes sobre una misma circunstancia, hace que los responsables de las operaciones puedan hacer su propia interpretación de los datos, e incluso se permite que los responsables introduzcan en el modelo sus propias percepciones de la situación basándose en los datos que llegan al sistema desde el campo de operaciones. Esta funcionalidad puede ser especialmente aplicable a labores de inteligencia de alto nivel.

La entidad REPORTING-DATA permite habilitar un mecanismo para mantener un histórico de información que puede ser aplicado no solo en el presente, sino que puede facilitar una buena base en la planificación de nuevas operaciones y movilización de recursos.

REPORTING-DATA se define como la especificación de la fuente de una información, su calidad y su tiempo de validez. La estructura de la entidad REPORTING-DATA incluye una relación obligatoria con la entidad ORGANISATION cuyo role es la identificación de las fuentes de información. Los dos subtipos de REPORTING-DATA sirven para especificar información temporal de los reportes de datos.

Las marcas temporales y los periodos de tiempo con significancia militar necesitan ser especificados dentro del modelo, por ejemplo el instante de comienzo de una operación, la hora de llegada de un reporte o la duración efectiva de una predicción metereológica. También se debe tener muy en cuenta la especificación de un tiempo como fijo (absoluto) con respecto a un calendario estándar o relativo con respecto a un origen arbitrario, por ejemplo día D+3.

Las características relativas o absolutas del tiempo se capturan en las dos entidades subtipo de la entidad REPORTING-DATA. Estas entidades subtipo son REPORTING-DATA-ABSOLUTE-TIMING y REPORTING-DATA-RELATIVE-TIMING.

REPORTING-DATA-ABSOLUTE-TIMING se define como un REPORTING-DATA que especifica una fecha y tiempo efectivos referidas a un calendario universal. Las fechas siguen el calendario gregoriano y las horas se definen en un formato de 24 horas respecto al tiempo universal.



REPORTING-DATA-RELATIVE-TIMING se define como un REPORTING-DATA que especifica un tiempo efectivo, que hace referencia a una instancia específica de la entidad ACTION-TASK. Tiempos relativos solo tiene sentido operacional en relación con actividades ya planeadas, en las que se define el origen de tiempos respecto del cual los tiempos relativos tienen sentido.

El modelo C2IEDM permite también el almacenar información de fuentes externas a la estructura de datos, como pueden ser mensajes ADatP-3, correos electrónicos impresos, transcripciones de llamadas telefónicas, etc. Toda esta información se almacena a través de la entidad REFERENCE que está asociada a REPORTING-DATA.

La vista completa de la estructura asociada a la entidad REPORTING-DATA se puede ver en la figura 29.

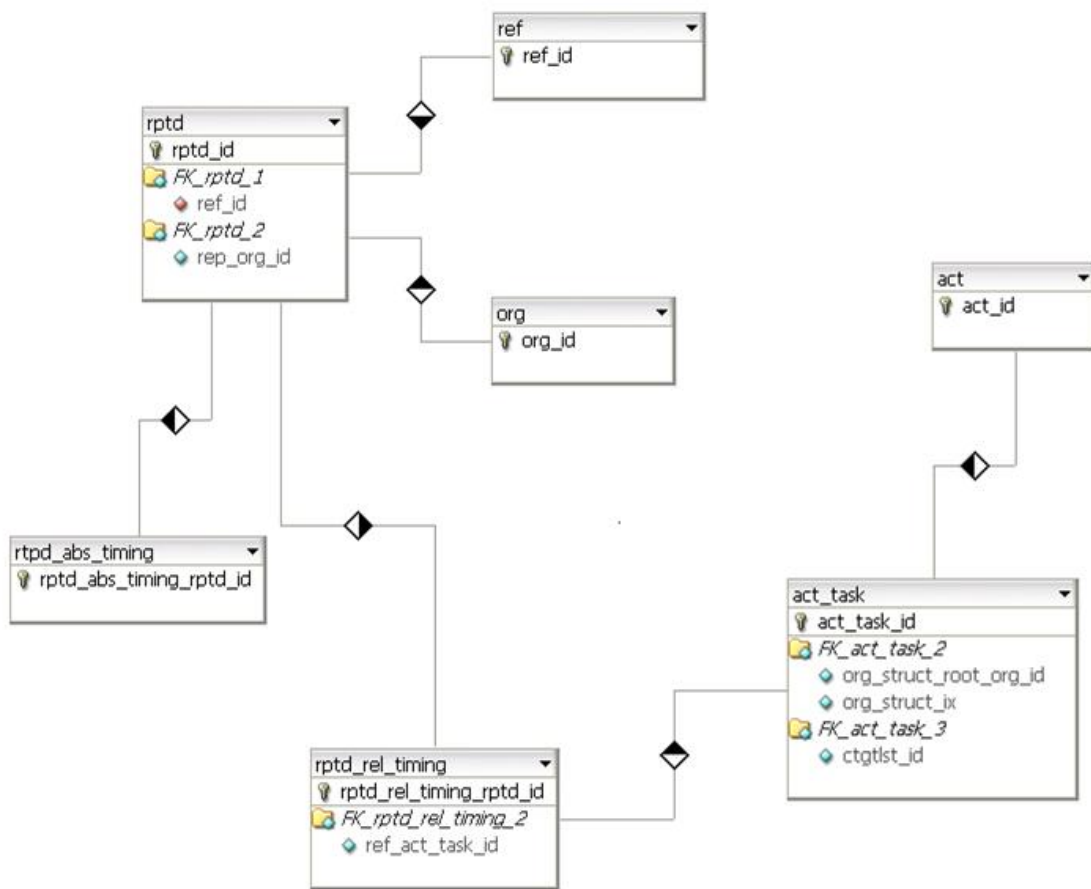


Figura 29

El hecho de que la entidad REPORTING-DATA este relacionada con muchas de las entidades del modelo presenta la oportunidad de combinar la información de formas muy complejas. El C2IEDM facilita este mecanismo de agrupación a través de la entidad independiente CONTEXT.

La entidad independiente CONTEXT puede ser usada para agrupar datos sin crear nueva información, esto puede implicar crear unas colecciones de datos relevantes para la situación o los entornos de algunas actividades o unidades.

De esta forma se pueden especificar condiciones que deben preceder a una determinada acción o que deberían resultar de la ejecución de una acción. Los planificadores de acciones pueden usar la información de CONTEXT para juzgar los meritos de un plan operacional y hacer los cambios correspondientes para poder responder a un cambio de la situación operacional.

La agrupación de información a través de CONTEXT puede ayudara gestionar la información dinámica ayudando a prevenir perdidas de información significativa que puede no ser reconocida como tal si no esta relacionada directamente con la descripción de la situación.

La vista completa de la estructura asociada a la entidad CONTEXT se puede ver en la figura 30.

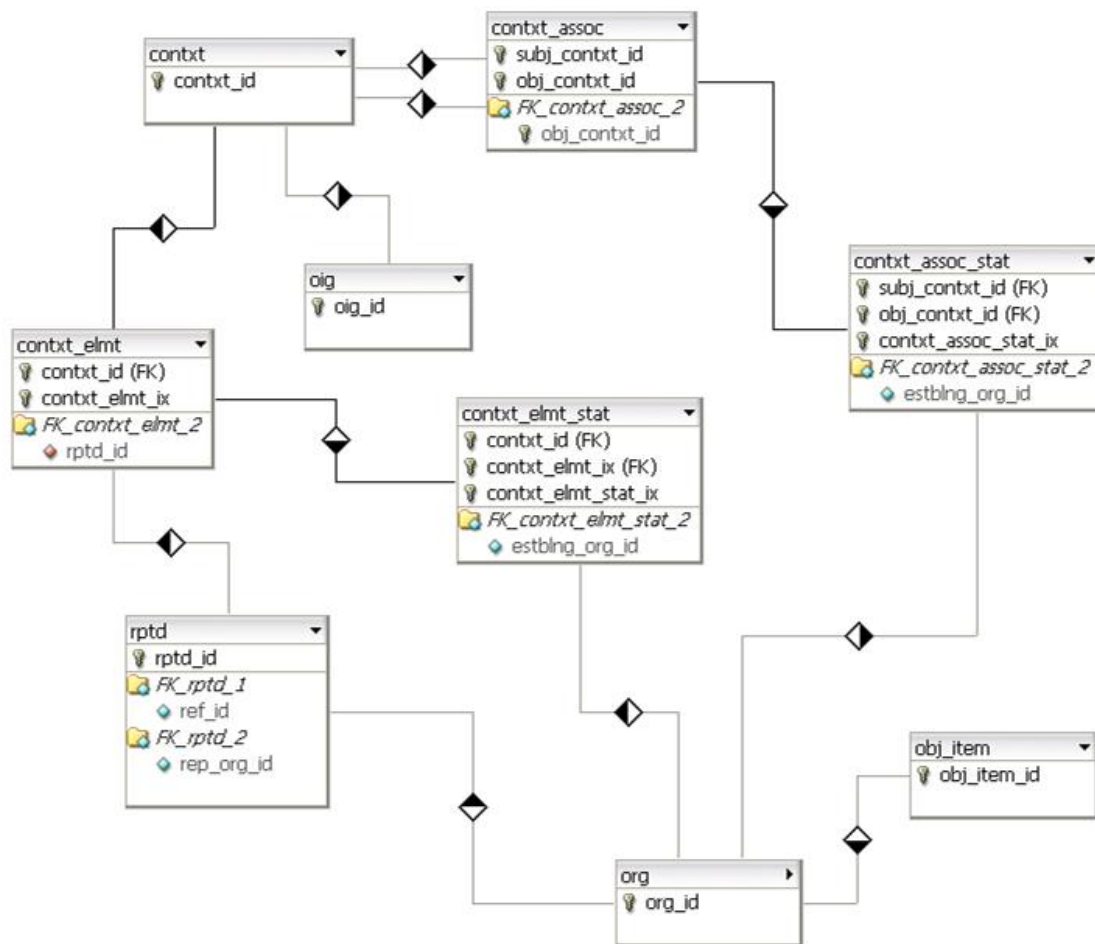


Figura 30

Los datos asociados con una instancia de la entidad CONTEXT se definen a través de la entidad CONTEXT-ELEMENT. La entidad CONTEXT-ELEMENT-STATUS mantiene un seguimiento del estado y de los tiempos de las instancias de CONTEXT-ELEMENT, de esta forma se preserva la integridad de los datos mientras se permite que el contenido de los datos cambie para cada instancia de CONTEXT.

La entidad CONTEXT-ASSOCIATION y su entidad hija CONTEXT-ASSOCIATION-STATUS, permiten relacionar una instancia de CONTEXT con otra con la relación definida por el valor del atributo “category code” en la entidad CONTEXT-ASSOCIATION.

### 3.4 Implementación del esquema físico del J3CIEDM Ed 3.0

En este apartado se va a describir la implementación del esquema físico de otro de los modelos de datos analizados, el J3CIEDM Ed 3.0, con objeto de poder llevar a cabo la investigación en la que se basa la presente tesis doctoral y poder realizar pruebas de interoperabilidad entre sistemas de mando y control, que nos ayudarán a formular las conclusiones de esta tesis doctoral.

El objetivo de este apartado es mostrar las principales categorías de información cubiertas por el modelo J3CIEDM Ed 3.0, que son de interés para los usuarios operacionales del modelo.

En primer lugar se mostrarán las 241 tablas de la base de datos implementada, junto con todas sus relaciones, las cuales representan a las 241 entidades con sus 1729 atributos que componen el J3CIEDM Ed 3.0.

En la figura 31 se pueden ver las 241 tablas que componen la base de datos que implementa el esquema físico del J3CIEDM Ed 3.0. Como gestor de bases de datos se ha utilizado el programa MySQL Administrator versión 4.1.12.

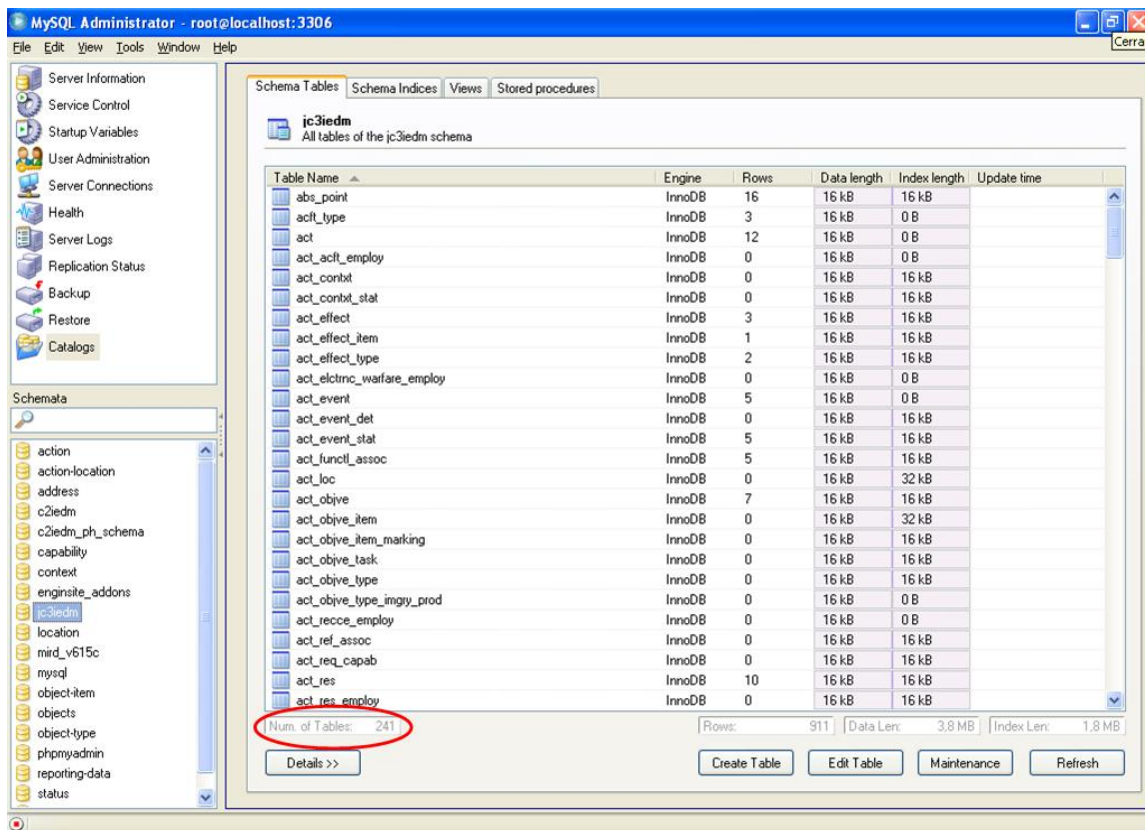


Figura 31

En la figura 32 se pueden ver los 359 índices que componen todas las relaciones entre las distintas entidades del modelo J3CIEDM Ed 3.0.

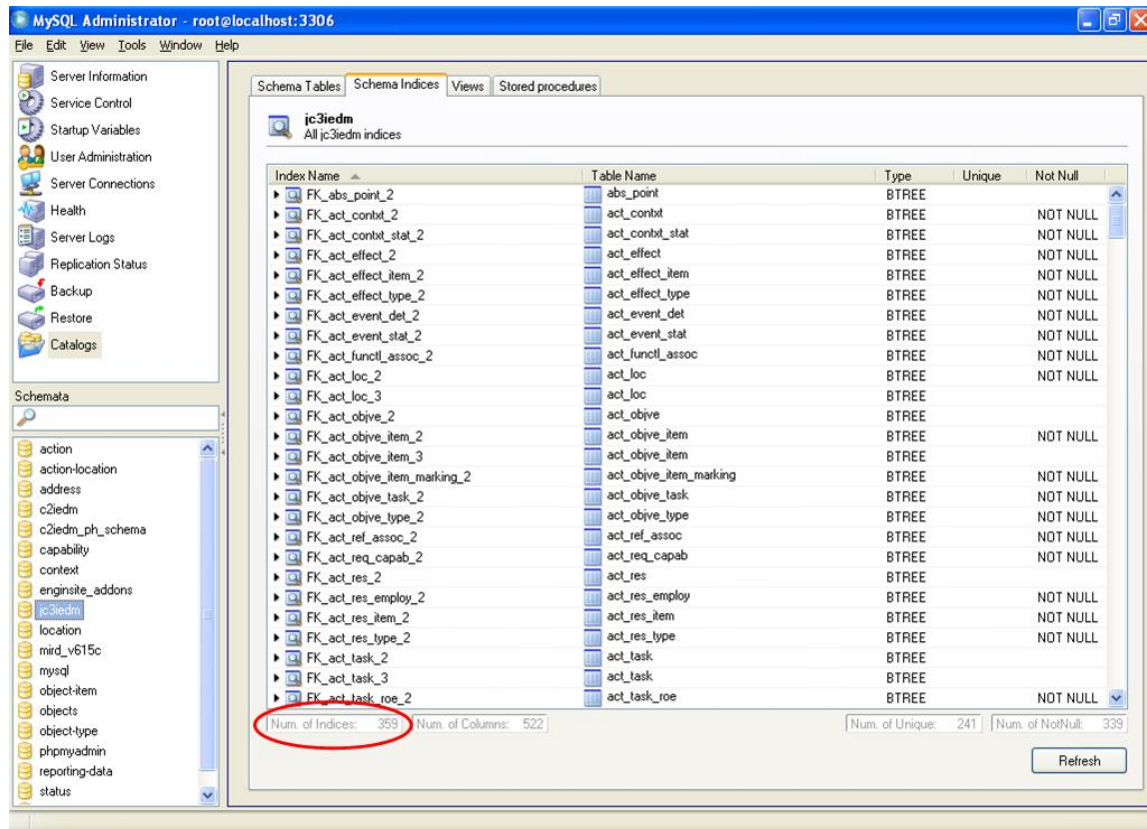


Figura 32

Como ya se dijo en el apartado 2.6.3 de la presente tesis doctoral, donde se describió la implementación del esquema físico del modelo C2IEDM v6.15c, no existe un camino lineal que pueda ser seguido de forma lógica, a través de todas sus entidades, para revisar un modelo de datos táctico como el L3CIEDM Ed 3.0.

El gran número de relaciones que existen entre las distintas entidades del esquema relacional hace que casi cada parte del modelo dependa de otras partes del mismo, por este motivo, en el presente apartado se va a organizar la estructura del modelo de datos de una forma que sea lo más descriptiva y clara posible para el lector.

Con este fin, se va a dividir la estructura lógica del modelo en cuatro partes claramente diferenciadas:

1. Objetos de interés y sus propiedades inherentes
2. Situaciones pasadas, presentes o futuras representadas por actos sobre los objetos
3. Actividades pasadas, presentes o futuras en las que los objetos están involucrados
4. Mecanismos para agrupar datos en paquetes de información.

Dentro de estas cuatro partes en las que se ha dividido la estructura lógica del modelo, se pueden describir las principales estructuras de datos del modelo. El significado y la utilización de las principales estructuras de datos del J3CIEDM Ed 3.0 son muy similares a las estructuras de datos, que ya se describieron con detalle en el apartado 2.6.3 de la presente tesis doctoral, donde se describió con detalle la implementación del esquema físico del modelo C2IEDM v6.15c.

Por este motivo y para evitar una descripción redundante de estructuras y conceptos muy similares, en este apartado se van a describir con detalle por una parte, solo aquellas estructuras de datos del J3CIEDM Ed 3.0 que hayan cambiado significativamente con respecto a su estructura homóloga del C2IEDM v6.15c o por otra parte, aquellas estructuras, que hayan sido introducidas por primera vez en el J3CIEDM Ed 3.0 y que no aparecieran en la implementación del esquema físico del C2IEDM v.615c.

Una estructura básica del modelo J3CIEDM Ed 3.0 y que ha cambiado de forma significativa con respecto a su estructura homóloga en el C2IEDM v6.15c es la estructura que representa la jerarquía completa de la entidad OBJECT-ITEM.

Las principales diferencias entre estas dos estructuras del objeto OBJECT-ITEM en ambos modelos se pueden ver señaladas dentro de la figura 31, que representa la estructura de OBJECT-ITEM en el modelo J3CIEDM Ed 3.0.

La primera diferencia que podemos ver en la parte superior derecha de la figura 31, es la adición de la entidad OBJECT-ITEM-ALIAS dependiendo directamente de la entidad OBJECT-ITEM. Esta entidad no aparece en el modelo C2IEDM v6.15c.

En la parte superior izquierda de la figura 31 podemos ver la independencia de las entidades ANCHORAGE, BASIN, BERTH, DRY DOCK, JETTY, QUAY, SLIPWAY con respecto de la entidad HARBOUR, lo que implicó el cambio de nombre de todas ellas y su dependencia directa de la entidad FACILITY.

Otra diferencia significativa que puede observarse en la figura 31 es la desaparición de las entidades MASS-GRAVE y MASS-GRAVE-CONTENT del modelo.

En la parte inferior de la figura 31 podemos destacar la adición de la entidades MINEFIELD-LAND, MINEFIELD-MARITIME, MINEFIELD-MARITIME-CASUALTY-ESTIMATE, MINEFIELD-MARITIME-SUSTAINED-THREAT-MEASURE-OF-EFFECTIVENESS al modelo dependiendo las dos primeras de la entidad MINEFIELD y las dos últimas de la entidad MINEFIELD-MARITIME.

Por último cabe destacar en la parte inferior izquierda de la figura 31 la adición de las entidades AIRSPACE-CONTROL-MEANS, APPROACH-DIRECTION, ROUTE-SEGMENT, AIR-ROUTE-SEGMENT, las tres primeras entidades dependientes de la entidad CONTROL-FEATURE y la última entidad mencionada dependiente de la entidad ROUTE-SEGMENT.

Los cambios en la estructura de la entidad OBJECT-ITEM mencionados anteriormente se muestran en la figura 33

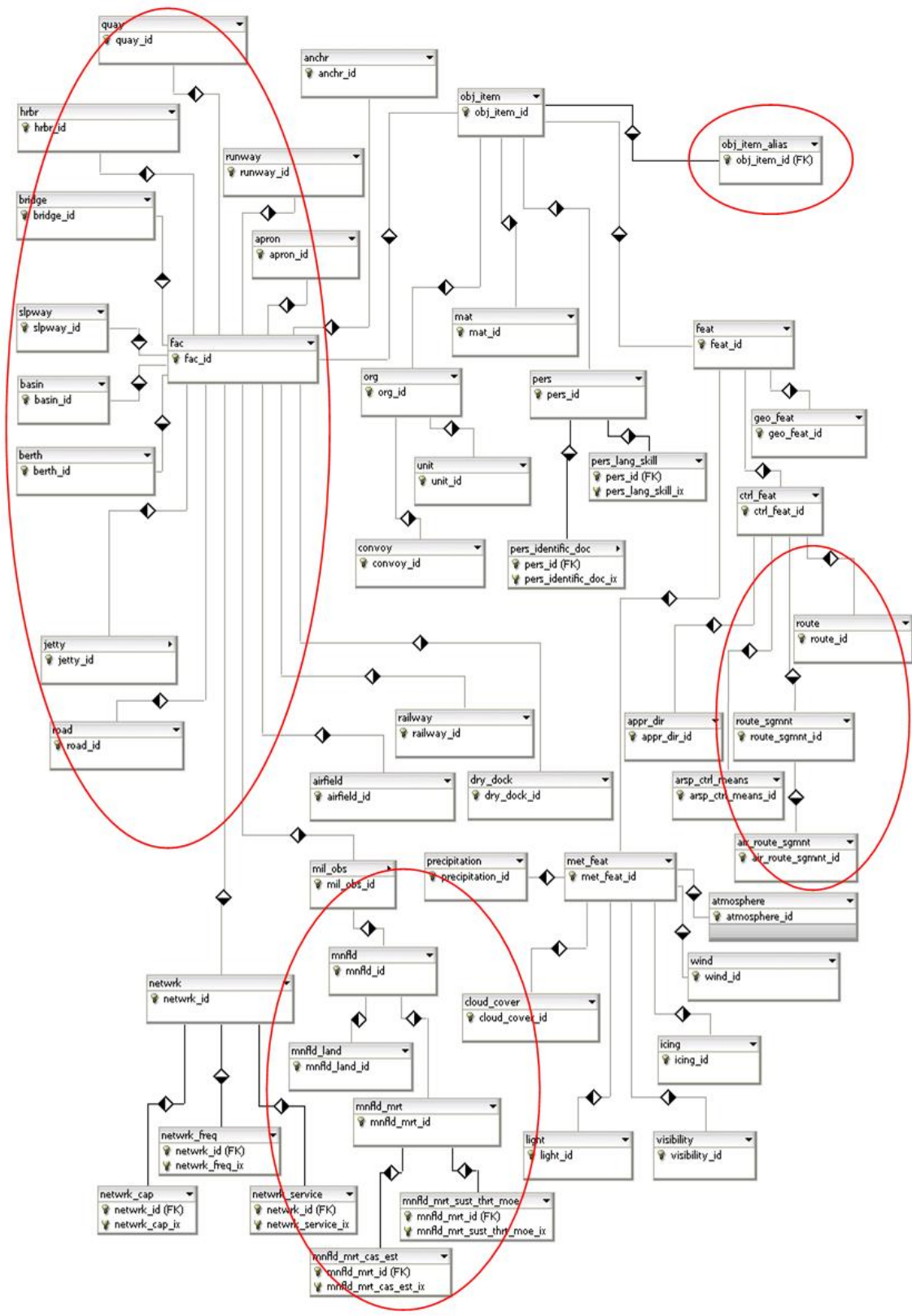


Figura 33

La segunda estructura de datos que se va a describir en este apartado por haber sufrido considerables modificaciones con respecto a su estructura homóloga del modelo C2IEDM v6.15c es la estructura que representa la jerarquía de la entidad ACTION.

La principal diferencia que presenta la estructura de la entidad ACTION en el J3CIEDM Ed 3.0 es la adición de las entidades CHEMICALBIOLOGICAL-EVENT, RADIOACTIVE-EVENT, NUCLEAR-EVENT, RADIOLOGICAL-EVENT y NUCLEAR-WEAPON-EVENT dependientes de la entidad CBRN-EVENT. Estos cambios vinieron provocados en respuesta a requerimientos relacionados con operaciones aéreas, temas relacionados con CBRN (Chemical, Biological, Radiological and Nuclear) y mejora de las especificaciones de la entidad ACTION

Estos cambios en la estructura de la entidad ACTION se muestran en la figura 34

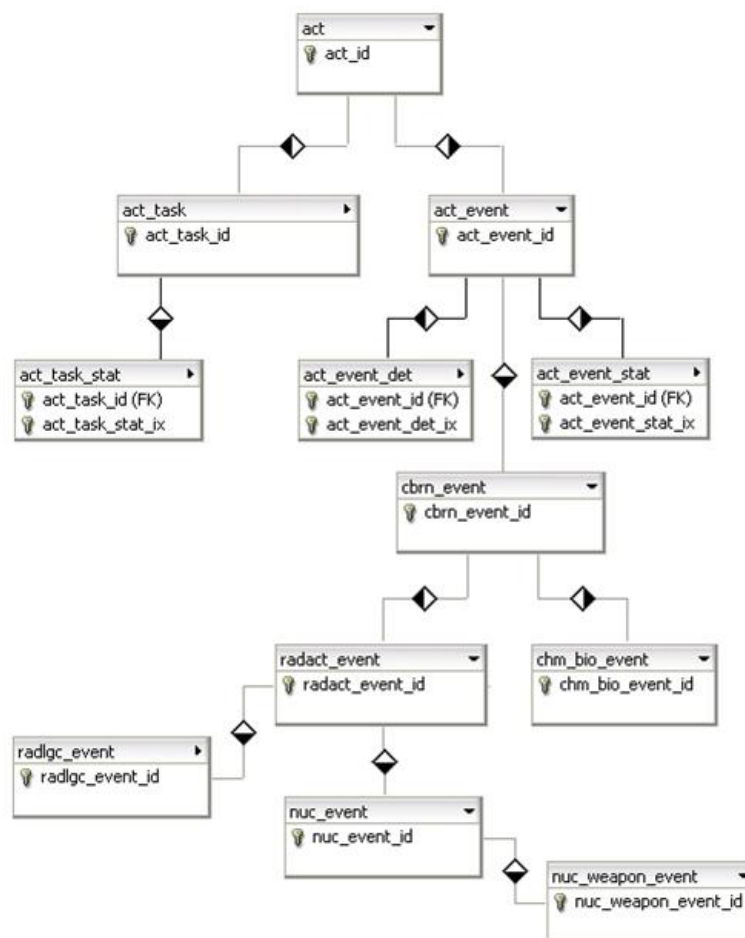


Figura 34

Por último en la figura 35 podemos ver los cambios en la estructura jerárquica de la entidad OBJECT-TYPE, en la parte superior derecha de la figura 35 se señala la adición de la entidad ROUTE-TYPE, dependiente de la entidad CONTROL-FEATURE. En la parte superior izquierda de la figura 35 se puede ver la adición de la entidad AIRFIELD-TYPE, dependiente de la entidad FACILITY-TYPE.



Los cambios en la estructura de la entidad OBJECT-TYPE mencionados anteriormente se muestran en la figura 35.

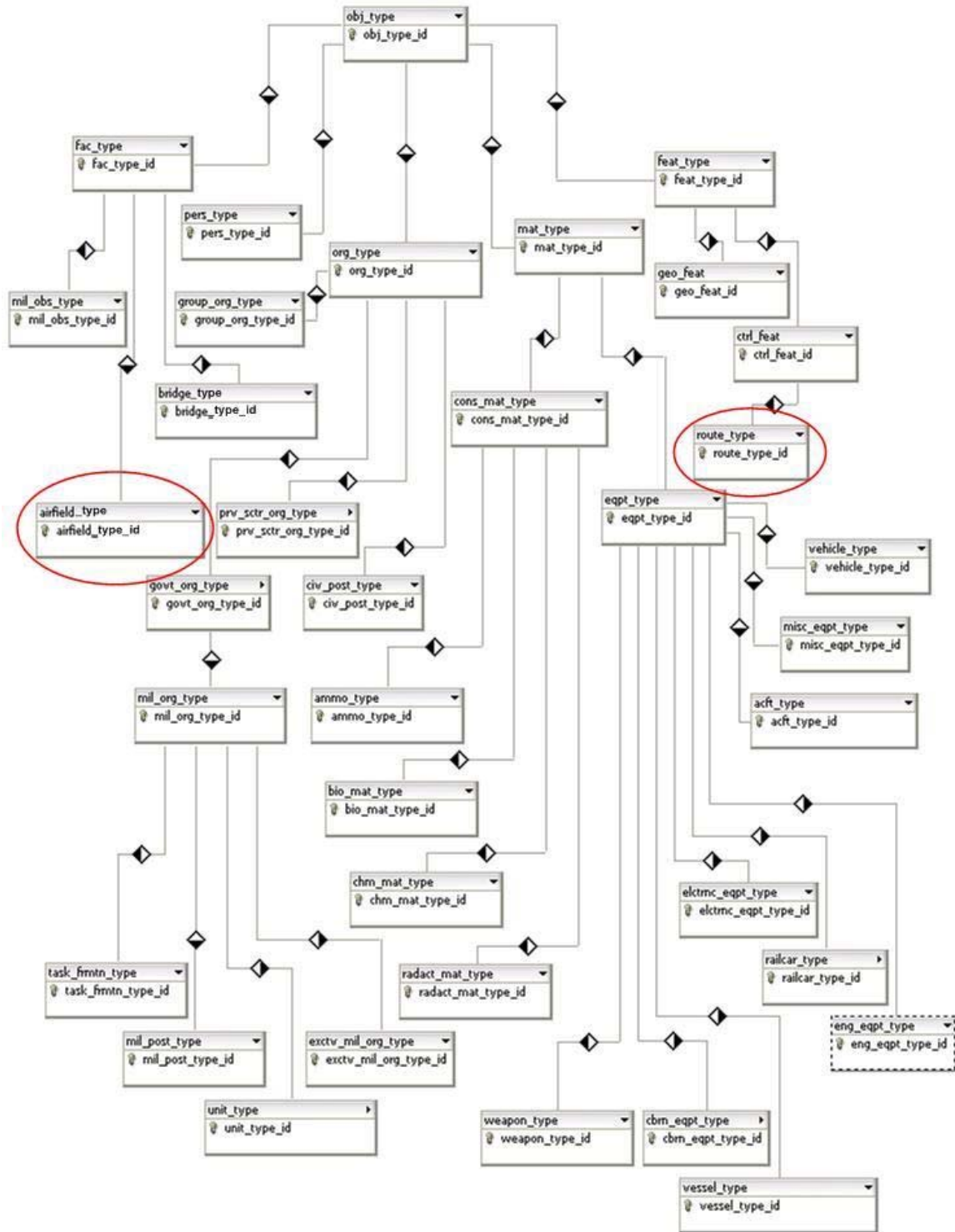


Figura 35

### **3.5 Interoperabilidad entre sistemas de mando y control**

Continuando con el cumplimiento de los objetivos expuestos en el apartado 1.2 de la presente tesis doctoral, en este apartado se van a describir los principales soluciones que permiten la interoperabilidad entre sistemas de mando y control militares y que han sido adaptados e implementados, como parte de la investigación llevada a cabo en la presente tesis doctoral, para ser probados como solución de interoperabilidad del sistema de seguimiento de fuerzas amigas o Friendly Force Tranking (FFT) que se va a analizar dentro de esta tesis.

En este apartado básicamente se van a describir dos soluciones de interoperabilidad y sus respectivas implementaciones, que han servido para facilitar distintas plataformas de interoperabilidad para los sistemas de mando y control y de seguimiento de fuerzas amigas, que se van a proponer en los siguientes apartados de esta tesis, como solución para la adaptación de los sistemas de mando y control y de los modelos de datos tácticos a la gestión de emergencias en el ámbito civil.

Las soluciones de interoperabilidad que se van a describir en este apartado son la solución desarrollada por el programa MIP y la solución basada en la utilización del estándar Nato Friendly Force Information (NFFI).

#### **3.5.1 Descripción e implementación de la solución MIP**

En este apartado se estudiará la descripción del mecanismo de intercambio de información para conseguir la interoperabilidad de sistemas, propuesto por el programa MIP.

La especificación del MIP consiste en un interfaz común de datos y en mecanismos de intercambio de información. El interfaz común es el C2IEDM, el cual modela la información que los sistemas de mando y control e información aliados necesitan intercambiar, tanto horizontalmente como verticalmente.

Los mecanismos de intercambio de información entre sistemas de mando y control e información, que el programa MIP ha especificado son los siguientes:

- El mecanismo de intercambio de mensajes (Message Exchange Mechanism, MEM) [42], que consiste en una serie de mensajes formateados que se ajustan al sistema AdatP-3 parte 1 [18], así como unas guías para su uso.
- El mecanismo de intercambio de datos (Data Exchange Mechanism, DEM) [42], que es un mecanismo automático de envío de datos y que coexiste con el MEM. Cuando una aplicación de mando y control cambia el estado de alguna información que ella mantiene o controla, esto es detectado por el DEM y la información en cuestión es automáticamente replicada en todos los sistemas de mando y control que están cooperando y que han acordado el intercambio de este tipo de información.

Con estos mecanismos de intercambio de información tanto el significado como el contexto de la información son mantenidos y por lo tanto, no se requiere ningún procesado adicional en recepción.

La especificación MIP habilita una interoperabilidad de nivel 4.a [43] para el DEM, una interoperabilidad de nivel 2.h [44] para el MEM y funciones de nivel 5 OTAN [45] para la interconexión de sistemas.

El MEM y el DEM tienen un periodo de plena vigencia de 2003 a 2005 y serán revisados a partir de esa fecha con mejoras que tendrán a su vez una vigencia bianual.

Una vez enunciados los mecanismos propuestos por MIP para conseguir la interoperabilidad de sistemas de mando y control e información vamos a estudiarlos en detalle.

### **3.5.1.1 La base de datos MIRD (Mip Information Resource Dictionary)**

La especificación MTIDP [42] (MIP Technical Interface Design Plan) implementa el mecanismo de intercambio de información entre sistemas de mando y control a través de un interfaz único, el C2IEDM. Dentro de esta especificación se incluyen los mecanismos MEM y DEM anteriormente mencionados.

La principal aplicación que permite la interoperabilidad entre sistemas de mando y control es el DEM, esta aplicación se gestiona a través de la base de datos de gestión MIRD (Mip Information Resource Dictionary), asociada a cada versión del interfaz común de datos (C2IEDM).

La base de datos MIRD o DEMS (Data Exchange Mechanism Schema), describe toda la información de gestión relevante para establecer el mecanismo de réplica, información sobre los nodos involucrados en las réplicas, entidades y atributos del interfaz de datos, filtros, etc.

La base de datos MIRD la podemos dividir en dos vistas diferentes, en las cuales podemos encontrar entidades relacionadas de forma lógica. Estas dos vistas son las siguientes:

- Vista de replicación del mecanismo de intercambio de datos; Esta vista describe los datos de gestión, que están directamente involucrados en el proceso de réplica. En la vista de replicación se incluyen datos sobre los nodos, filtros, contratos y tipos de dominios de réplica (REPLICATION-DOMAIN-TYPEs).
- Vista del modelo de datos (Interfaz común de datos); En este subconjunto de la base de datos MIRD se encuentran datos relativos al interfaz de datos, sobre el cual se va a efectuar la réplica. Esta vista del modelo de datos incluye datos sobre entidades (tablas del modelo), atributos (columnas de dichas tablas) y sus relaciones. La vista del modelo de datos tiene las siguiente entidades en común con la vista de replicación: ENTITY, ATTRIBUTE, SUBJECT-VIEW, y VIEW-ENTITY.

El DEM además facilita mecanismos de intercambio de información operacional y de gestión controlados por el usuario y estructurados de acuerdo a la base de datos MIRD.

Los mecanismos de intercambio de información de gestión hacen, que dependiendo de su naturaleza, los datos de la base de datos MIRD puedan ser replicados junto con los datos operacionales del interfaz de datos común durante el desarrollo de una operación. Es decir, datos de gestión de tipo dinámico pueden ser replicados vía DEM en respuesta a eventos de gestión, como por ejemplo datos relacionados con la topología de la red, direcciones de nodos, nuevos nodos, etc.

En el caso de que los datos estáticos de la base de datos MIRD, estos son distribuidos fuera del DEM, por ejemplo en un CD.

Se asume que estos datos estáticos estarán presentes en la base de datos MIRD antes de empezar el proceso de réplica.

### **3.5.1.2 Descripción del mecanismo de réplica de datos DEM**

El mecanismo de réplica DEM distribuye la información operacional de una forma selectiva desde un nodo a otros nodos que desean recibir esos datos actualizados. La frase “de una forma selectiva” refleja el hecho que solo los datos que han sido requeridos por un receptor y que su dueño ha accedido a cederlos, serán transferidos durante el proceso de réplica.

Estos acuerdos entre receptores y proveedores de datos se materializan en contratos de réplica entre las dos partes implicadas. El DEM contiene la suficiente funcionalidad para asegurar que solo los datos requeridos son replicados a sus receptores.

El mecanismo de réplica una vez comienza es automático, pero en todo momento esta bajo el control de los usuarios o contratistas, este control online por parte del usuario es necesario para asegurar el nivel 5 OTAN de interconexión de sistemas [46], que impliquen necesidad de control dinámico sobre los datos que van a replicar, y sobre los nodos que van a recibir estos datos.

Todo esto se hace posible permitiendo que la base de datos MIRD, pueda ser actualizada durante las operaciones en curso, principalmente para ajustar el conjunto de datos replicados (Dominios de réplica y filtros) y el conjunto de proveedores y receptores de información (Actualización de suscripciones).

A continuación se va a describir la arquitectura del DEM, el esquema de dicha arquitectura se puede ver en la figura 36.

En la figura 36 se puede ver el tipo de funciones que facilita cada nivel de la arquitectura del mecanismo de replica del MIP. La figura especifica dos secuencias de acciones, una descendente y realizadas desde el proveedor de los datos o Data Provider (DP), a la izquierda de la imagen y una ascendente realizadas desde la parte del receptor de los datos o Data Receiver (DR), en la parte derecha.

La primera secuencia de acciones comienza cuando el sistema de mando y control o aplicación realiza una operación que origina una actualización en el núcleo común o interfaz de datos. Cuando esto se produce se chequea si los datos actualizados forman parte de la información susceptible de ser replicada en cualquiera de los contratos que se tienen activos en ese momento. Si la información actualizada aparece en algún contrato como susceptible de ser replicada se forman las unidades de datos del protocolo o Protocol Data Units (PDU), que son las unidades o paquetes mínimos de información que define el DEM y en ellos se introducen los datos.

En la parte central de la figura se pueden ver tres niveles de la arquitectura que hacen de interfaces entre el nivel de aplicación y el soporte de la transmisión, estos tres niveles son el gestor de la replicación (REPMAN), el gestor de la asociación (ASSOCMAN) y el gestor de la transmisión (TFMAN).

La principal tarea del nivel REPMAN es controlar los asuntos relacionados con la sincronización, determinando básicamente que elementos deben ser sincronizados para conectar las bases de datos de los sistemas implicados en la réplica y como deben ser sincronizados estos elementos, esta acción la realiza analizando y evaluando la información de los contratos en vigor entre dichos sistemas.

Otra de las funciones del REPMAN es generar mensajes durante la conexión para realizar un seguimiento de los estados de las bases de datos y de los nodos implicados en la réplica de datos. El REPMAN también ofrece un servicio para asegurar las entregas de los paquetes por medio de tiempos de espera y reenvíos.

El nivel ASSOCMAN tiene básicamente dos tareas: identificar los datos reenviados y mantener un orden de los paquetes enviados.

La tarea principal del nivel TFMAN es facilitar medios de comunicación entre los dos nodos implicados en el proceso de réplica. Para realizar esta tarea este nivel dispone de información de la disponibilidad de un número de varios soportes de transmisión, con esta información el TFMAN se encarga de seleccionar el soporte más adecuado para la proceder a la réplica y de los asuntos de direccionamiento relacionados con la conexión.

El nivel de soporte de la transmisión facilita una abstracción de los protocolos de red como TCP/IP ó X400 y de los servicios de red como compresión de la información, encriptado o corrección de errores.

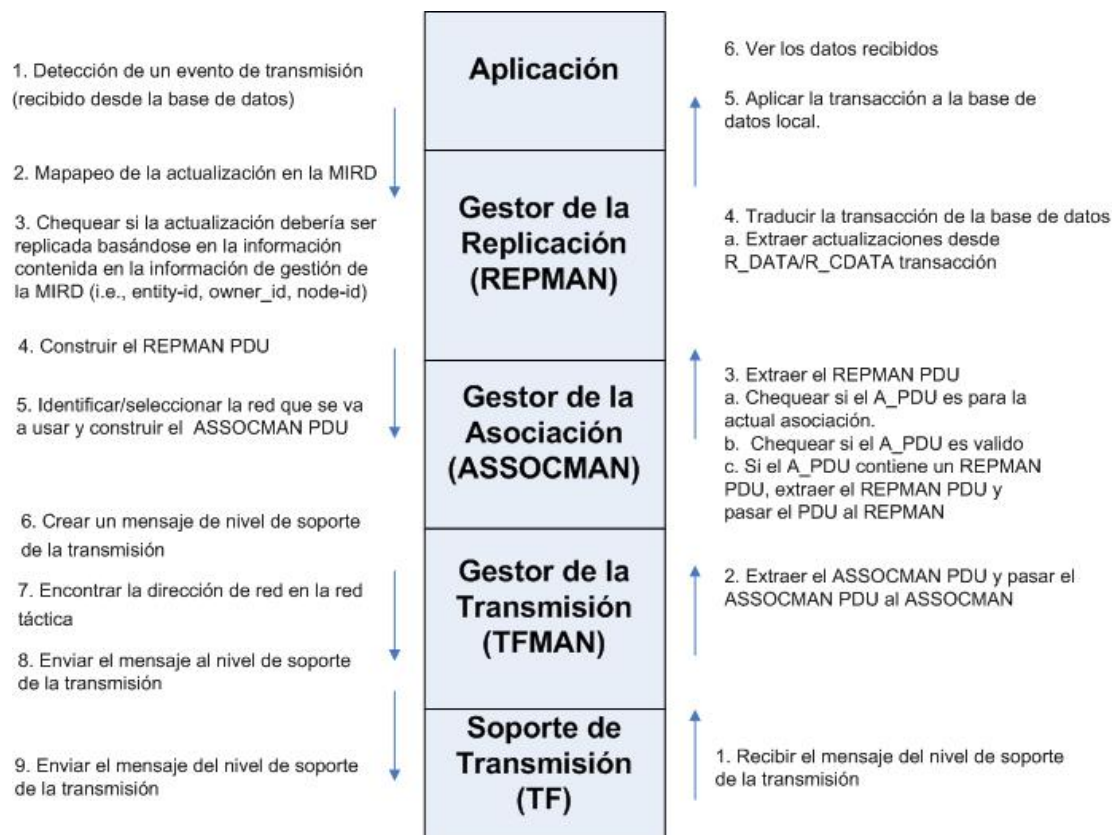


Figura 36

El elemento mínimo de información manejado por los cuatro niveles es la PDU. Dos ejemplos de PDUs que se pueden ver en la figura 36 son A\_DATA, el cual es transmitido entre los dos niveles ASSOCMAN y R\_DATA, el cual es transmitido entre los dos niveles REPMAN.

En la figura 36 también se describe la transmisión de datos operacionales y no solo de gestión de la conexión. En la siguiente secuencia se va a describir la forma en la que una PDU de datos operacionales o de gestión es encapsulada sucesivamente en cada nivel de la arquitectura:

Datos operacionales o de gestión: Ejemplo: X01 o G01 son empaquetados dentro de una R\_DATA PDU al llegar al nivel de REPMAN, Ejemplo: R05{X01}, luego son empaquetados dentro de una A\_DATA PDU: Ejemplo: A05{R05{X01}} y finalmente son empaquetados dentro de una TFMAN PDU para ser transmitidos, Ejemplo: T03{A05{R05{X01}}}

Existen numerosos tipos de paquetes asociados a eventos y a potenciales situaciones, que se pueden dar durante la transmisión de los datos replicados. Todos estos estados y sus paquetes asociados se verán en el siguiente apartado, donde se describirá la implementación que se ha realizado del mecanismo de réplica DEM como parte de la investigación llevada a cabo en la presente tesis doctoral con objeto de adaptar el concepto del núcleo o interfaz de datos común a la gestión de emergencias civiles.

### **3.5.1.3 Implementación del mecanismo de réplica de datos DEM**

Para poder implementar el mecanismo de réplica DEM, como parte del trabajo llevado a cabo dentro de la presente tesis, primeramente se implementó el esquema físico de la base de datos de gestión MIRD, asociada a la versión 6.15c del modelo C2IEDM [47]. Esta base de datos se puede encontrar en formato MS ACCESS en la página Web del programa MIP [10].

Esta base de datos ha sido completamente migrada al formato MySQL, con el fin de que pueda ser integrada con el interfaz común de datos, que se ha diseñado también como parte de la presente tesis, para implementar el mecanismo de réplica DEM y que esta basado en el modelo C2IEDM v6.15c.

La aplicación que se ha desarrollado para implementar la especificación del mecanismo de réplica DEM, utiliza la base de datos MIRD, en formato MySQL, como base de datos gestión de los procesos de réplica.

Esta base de datos está formada por 51 tablas y 190 relaciones distintas, a través de estas tablas se gestionará totalmente el proceso de la réplica automática de datos, que hará posible la interoperabilidad entre sistemas de mando y control y sistemas de seguimiento de fuerzas amigas (Friendly Force Traking, FFT). En la aplicación desarrollada, se ha dividido conceptualmente la base de datos MIRD en dos módulos principales, en los que se agrupan las tablas por su funcionalidad, dentro del proceso de transferencia y actualización de datos que se realiza durante la réplica.

En la figura 37 se pueden ver las 51 tablas que componen la base de datos que implementa el esquema físico de la base de datos MIRD asociada al interfaz de datos C2IEDM v6.15c.

Como gestor de bases de datos se ha utilizado el programa MySQL Administrator versión 4.1.12 [41].

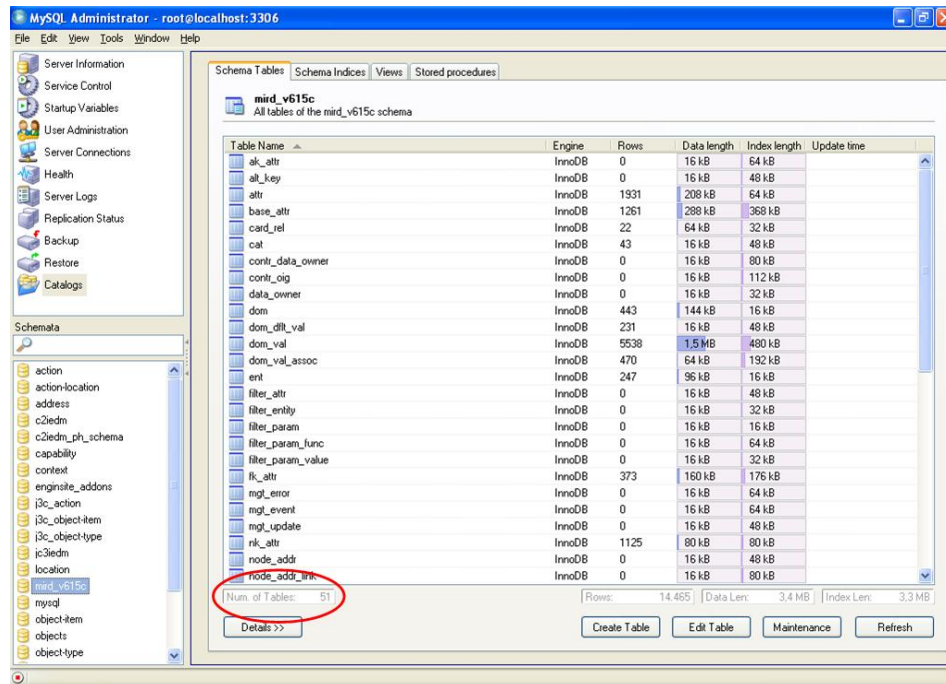


Figura 37

En la figura 38 se pueden ver los 190 índices, que componen todas las relaciones entre las distintas entidades de la base de datos MIRD asociada al modelo C2IEDM v6.15c.

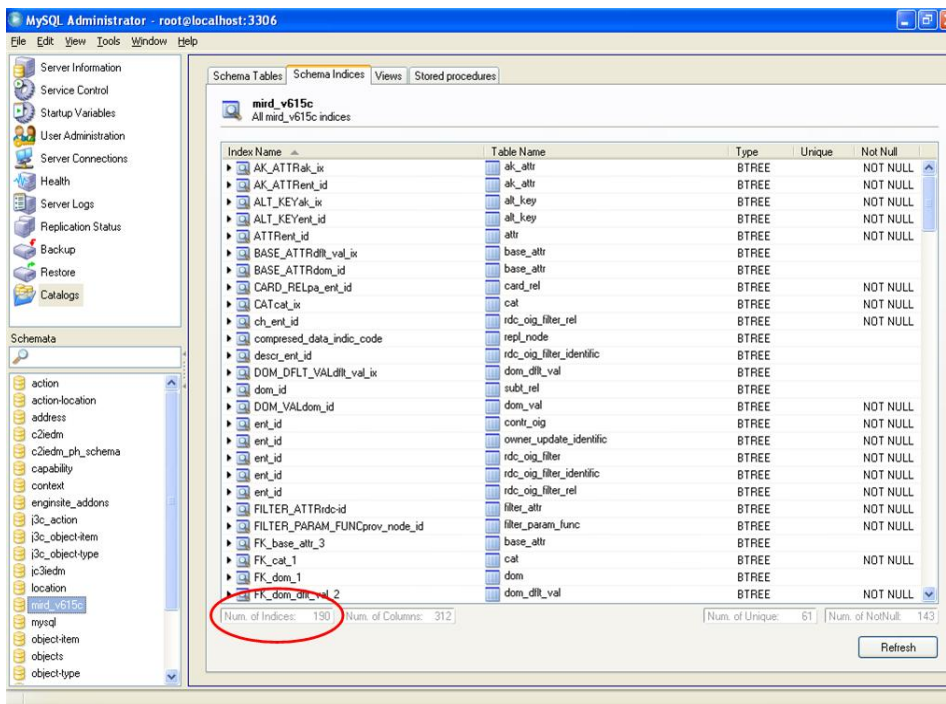


Figura 38







A continuación se exponen unas notas aclaratorias que ayudarán al entendimiento de los diagramas de estado;

Cada transición consta de un texto de dos o tres líneas, la primera línea indica el lanzamiento de un evento, si está escrito en minúsculas, o la llegada de una PDU, si esta escrita en mayúsculas. El resto de las líneas del texto explicativo de cada transición indica la respuesta del sistema al evento indicado en la primera línea.

CLOSING por el DR ó DP: indica que el iniciador del R\_Close\_req es el DR ó el DP de la presente sesión.

Si T1 expira, entonces se asume que el R\_Abort\_req que arma T1 ha fallado y se procede a abortar la asociación localmente.

Asunciones:

Las actividades descritas en el diagrama de estado son únicas en una sesión y su asociación relacionada.

Clarificaciones:

P1: Respuesta positiva

P2: Respuesta negativa

P3: Un asociación ya esta abierta en el presente nodo.

Acciones:

(1) Limpia el contexto de una sesión

(2) Descarta el mensaje

(6) Arma el temporizador (T1)

(11) Limpia el contexto local de la asociación relacionada

En los siguientes párrafos, una vez descrita la filosofía del mecanismo de réplica DEM, se describirá la arquitectura y el funcionamiento de la aplicación desarrollada, que implementa el mecanismo DEM en la presente tesis.

En la aplicación desarrollada para implementar la especificación del mecanismo de réplica DEM se pueden distinguir dos módulos principales;

El primer módulo es el módulo de conexión, el cual gestiona los protocolos de utilizados para establecer la conexión entre los nodos implicados y mantener dicha conexión mientras dure la sesión.

Este módulo se encarga de gestionar eventos lanzados por el sistema de mando y control que está replicando sus datos y de procesar las PDU's recibidas desde otros nodos. (Ver número 1 en figura 41)

Este módulo gestiona las siguientes tablas de la base de datos MIRD; REPLICATION-NODE, TRANSFER-FACILITY, REPLICATION-NODE-ADDRESS, REPLICATION-NODE-LINK, REPLICATION-NODE-ADDRESS-LINK, REPLICATION-ORGANISATION, y REPLICATION-NODE-MANAGER.

El segundo módulo de la aplicación de réplica que se va a describir, es el módulo de gestión de la réplica. Este módulo se encarga de gestionar la base de datos MIRD, entre sus funciones están la gestión de la propiedad de los datos, la gestión dinámica de los contratos con otros nodos, etc. (Ver número 2 en figura 41)

Este segundo módulo se puede dividir en varios submódulos, que gestionan a su vez distintas partes de la base de datos MIRD.

El primero de estos submódulos que se van a describir es el encargado de la gestión tanto de los contratos como del interfaz de datos (C2IEDM v6.15).

Este submódulo gestionará las siguientes tablas de la base de datos MIRD; REPLICATION-DOMAIN-COMPOSITE, REPLICATION-DOMAIN-COMPOSITE-ELEMENT, REPLICATION-DOMAIN-TYPE, REPLICATION-DOMAIN-TYPE-ELEMENT, REPLICATION-DOMAIN-COMPOSITE-FILTER, REPLICATION-DOMAIN-COMPOSITE-FILTER-ENTITY, REPLICATION-DOMAIN-COMPOSITE-FILTER-PARAMETER, REPLICATION-CONTRACT, CONTRACT-DATA-OWNER, REPLICATION-SUBSCRIPTION, REPLICATION-CONTRACT-FILTER-PARAMETER-FUNCTION, REPLICATION-CONTRACT-FILTER-PARAMETER-VALUE y REPLICATION-DOMAIN-COMPOSITE-FILTER-ATTRIBUTE.

Las siguiente cuatro entidades que se van a mencionar están más relacionadas con la gestión del interfaz de datos (C2IEDM v6.15c): ENTITY, ATTRIBUTE, SUBJECT-VIEW y VIEW-ENTITY.

El segundo submódulo que se va a describir es el encargado de la gestión de eventos. Este submódulo va a gestionar las siguientes tablas de la base de datos MIRD; MANAGEMENT-EVENT, MANAGEMENT-UPDATE y MANAGEMENT-ERROR. Estas tablas se usan para capturar cambios en la gestión de la réplica y en la gestión de los contratos.

El proceso de réplica implementado es totalmente automático y su descripción funcional es la siguiente:

Un programa demonio que monitoriza constantemente cualquier actualización del interfaz de datos común (C2IEDM), detecta automáticamente cualquier actualización en el interfaz común de datos (Ver número 3 en figura 41), posteriormente la aplicación de gestión de la réplica verifica si la información introducida o actualizada en el interfaz de datos está incluida en alguno de los contratos de réplica que están activos en ese momento en la base de datos MIRD, (Ver número 4 en figura 41), en caso afirmativo el proceso de réplica comienza de forma automática.

Como primer paso, sistema comprueba que se cumplen las condiciones para establecer la conexión con el nodo que actuaría como receptor de los datos (DR). En concreto, las condiciones que deben darse para establecer una conexión entre dos nodos son las siguientes;

- El atributo “status-code” de la tabla REPL-NODE debe tener el valor “AC” (Active), en el nodo proveedor de la información.
- El atributo “dst-node-link-status-code” de la tabla NODE-LINK debe tener el valor “AC”, en la entrada de la tabla del nodo proveedor.
- El atributo “status-code” de la tabla REPL-SUBSCR debe tener el valor “AC” (Active), si el nodo proveedor de la información es el nodo local.
- El atributo “status-code” de la tabla REPL-CONTR debe tener el valor “AC” (Active), si el nodo proveedor de la información es el nodo local.
- El atributo “status-code” de la tabla REPL-NODE debe tener el valor “AC” (Active) o “MA” (Management), en el nodo receptor de la información.
- El atributo “dst-node-link-status-code” de la tabla NODE-LINK debe tener el valor “AC”, en la entrada de la tabla del nodo receptor

Todas estas condiciones se verifican en la base de datos de gestión MIRD por la aplicación de gestión de la réplica.

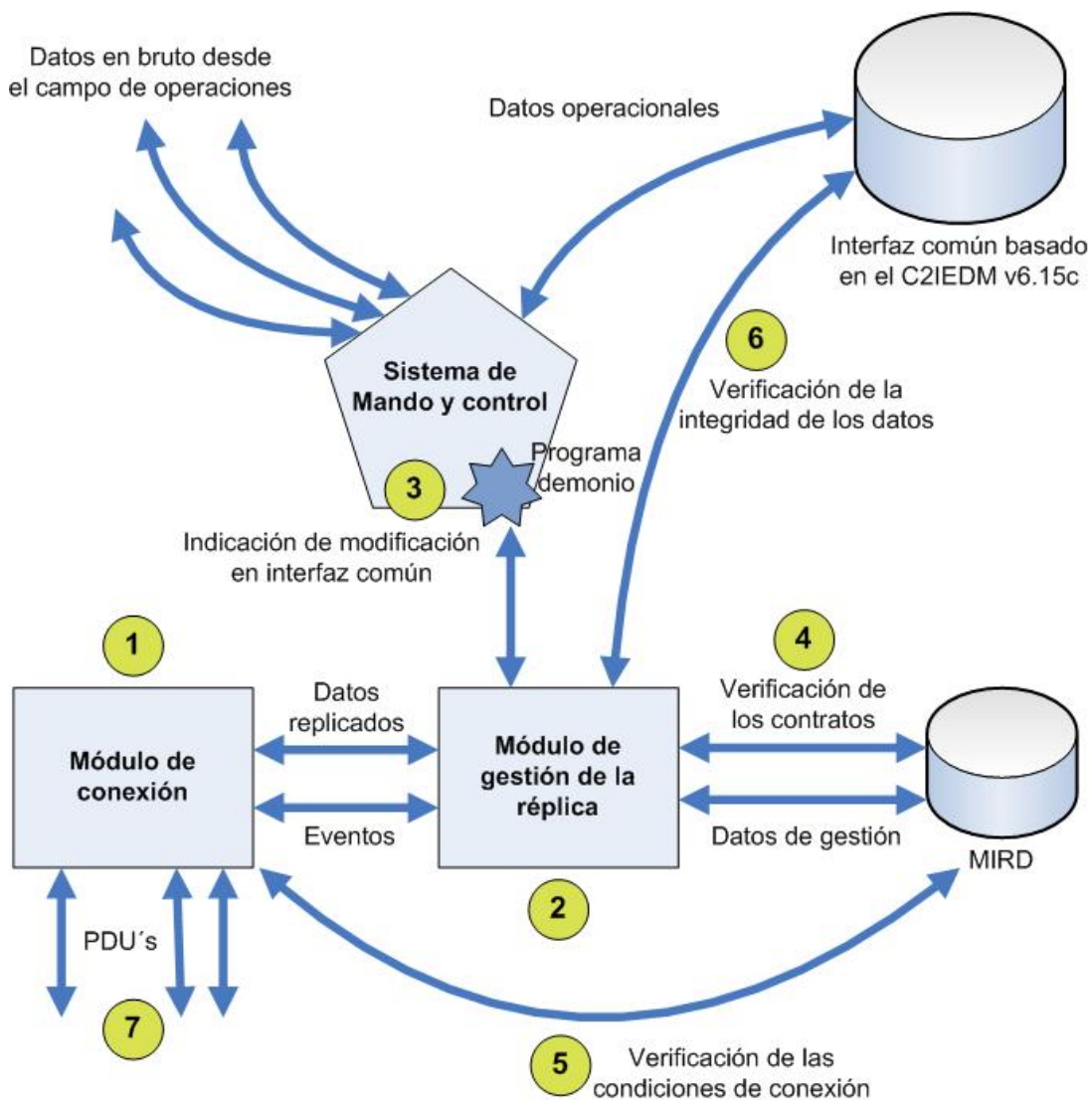
Una vez verificadas las condiciones expuestas anteriormente, si todas son correctas, se establece la conexión con el nodo receptor de la información que se va a replicar, esta conexión se establecen a través de la información que se encuentra en las siguientes tablas de la base de datos MIRD: REPLICATION-NODE, REPLICATION-NODE-LINK, TRANSFER-FACILITY, REPLICATION-NODE-ADDRESS y REPLICATION-NODE-ADDRESS-LINK. Estas tablas son gestionadas por el módulo de conexión. (Ver número 5 en figura 41).

Cuando la conexión se ha establecido con éxito, se verifica que los datos que van a ser replicados mantienen su integridad dentro del interfaz común de datos, es decir, no solo replican los datos actualizados sino todos aquellos que hacen que la integridad general de la base de datos receptora se mantenga de forma correcta.

Para esto se seleccionan los datos adicionales que sean necesarios para el mantenimiento de la integridad de la información que se va a replicar y se incluyen en la información que se replica al nodo receptor (Ver número 6 en figura 41).

Una vez asegurada la integridad de los datos, comienza el intercambio de mensajes (PDU's) (Ver número 7 en figura 41), entre el nodo proveedor y el receptor hasta completar totalmente el proceso de réplica establecido en su contrato.

El proceso completo de réplica que implementa la aplicación desarrollada y la secuencia de acciones a tomar para completar dicho proceso se muestran en la figura 41.



**Figura 41**

La aplicación desarrollada permitirá el proceso de réplica de datos entre dos sistemas C2IS que contengan el mismo interfaz común de datos, en este caso el C2IEDM v6.15c, en sus bases de datos respectivas.

Una vez probada la aplicación de réplica en el laboratorio con resultados satisfactorios, se procedió a su integración en el sistema de mando y control propuesto por la presente tesis doctoral para su uso en gestión de crisis civiles.

Cabe destacar que la complejidad que la aplicación de réplica implementada presenta es elevada, ya que implementa por completo el estándar DEM del programa MIP. Esta complejidad se reduce considerablemente al ser integrada en el sistema propuesto, ya que su interfaz común de datos, que ha sido desarrollado como parte de las investigaciones de la presente tesis, es mucho menor que el C2IEDM v6.15c, aunque esta basado en él. El interfaz de datos diseñado e implementado durante esta tesis se expondrá en detalle en apartados posteriores de la misma.

Todo el proceso de réplica se ha probado tanto utilizando redes cableadas Ethernet 100BaseT, como redes inalámbricas que cumplen el estándar IEEE 802.11 a/b/g (WIFI) [48].

### **3.5.1.4 Descripción e implementación del estándar NFFI**

Las primeras investigaciones que dieron lugar al estándar para la interoperabilidad de sistemas de seguimiento de fuerzas amigas de la OTAN ó NATO Friendly Force Information (NFFI), se iniciaron en 2005 y continuaron durante 2006 bajo el programa experimental de trabajo de las agencias de mando, control y consulta de la OTAN ó NATO Consultation Command and Control Agencies (NC3A) [49] Experimental Programme, y el programa científico de trabajo para la transformación del mando aliado ó Allied Command Transformation (ACT).

Estas investigaciones dieron lugar, el 21 de septiembre de 2006, al primer draft del STANAG 5527 [50], el cual está basado en la versión 1.3 del NFFI [51].

El seguimiento de fuerzas amigas normalmente hace referencia al reporte, de forma automática y cooperativa, de datos de posicionamiento de las unidades amigas a través de sistemas llamados sistemas de seguimiento de fuerzas o Force Tracking Systems (FTS).

Las unidades que son objeto de seguimiento son típicamente vehículos o unidades de tropa a pie, aunque también se puede plantear, por parte de la fuerza aérea, el seguimiento de un avión a través de un sistema FTS. El seguimiento de fuerzas enemigas debería ser una funcionalidad que podría ser soportada por los sistemas FTS en un futuro.

Se prevé que el peso y el papel de los sistemas FTS se incremente de forma exponencial en un futuro cercano, por este motivo el conseguir la interoperabilidad entre los sistemas FTS de las diferentes naciones se considera un objetivo crítico por parte de la OTAN. Por esta razón el programa NFFI intentó agrupar el mayor número de naciones, de sistemas nacionales y de expertos posible dado la importancia del objetivo.

La completa automatización en el procesado de la localización de las fuerzas amigas por un sistema F(Friendly)FTS es casi una realidad y lo será por completo en breve, la actividad humana se limitará exclusivamente a la gestión, configuración y funciones de control del sistema.

Es de suponer que los datos de localización se generarán automáticamente desde los dispositivos del FTS colocados en las unidades, el uso del NFFI se circunscribe a los datos que estos dispositivos pudieran generar de forma automática, datos que debieran ser introducidos manualmente en el sistema no serían considerados por el estándar NFFI.

Esta omisión de la intervención humana en el reporte de información es nueva en sistemas orientados a operaciones terrestres, pero ya es usada en sistemas de reportes de información marítimos y aéreos, como por ejemplo ADatP-3.

La introducción de datos generados por sensores dentro del NFFI se revisó y se extendió de acuerdo a la experiencia ganada durante los experimentos del programa CWID.

Por todo lo expuesto anteriormente se puede afirmar que el objetivo principal del programa NFFI a corto y medio plazo, es lograr la interoperabilidad de los sistemas FFTS nacionales en las futuras operaciones conjuntas en las que intervengan este tipo de sistemas de seguimiento y posicionamiento [52].

El proceso de diseño y modelado de datos usado para definir el mensaje NFFI fue el siguiente:

El primer paso que se dio en este proceso fue el integrar un número de definiciones de conceptos considerados clave y que ya se aplicaban o eran usados en los sistemas FTS existentes.

Datos que fueron considerados aplicables para su uso en los sistemas FTS, fueron agrupados en secciones que constituyen el mensaje NFFI. Se tuvieron en cuenta dos factores clave cuando se realizó el análisis de los datos.

- Relaciones lógicas y/o funcionales y afinidad entre los datos candidatos.
- Caracterización de seguridad; se asumió que diferentes secciones del mensaje NFFI podrían tener diferentes clasificaciones de seguridad. Por lo tanto en una operación multinacional la selección de elementos en las diferentes secciones del mensaje tendrá un impacto sobre la cantidad de datos que se van a intercambiar entre los distintos dominios de seguridad.

La decisión final sobre la bondad y la aplicabilidad del modelo de datos se basó en los resultados de los experimentos realizados. Estos experimentos fueron realizados a través del programa CWID.

El siguiente paso fue la identificación de las fuentes de información reales y su caracterización dentro de las principales fuentes de información previamente definidas. El análisis de la problemática de la interoperabilidad entre sistemas FTS, un análisis de los sistemas FTS existentes, así como un conjunto de experimentos llevados a cabo dentro del programa CWID, facilitaron a la NC3A resultados muy valiosos para seleccionar las definiciones de fuentes de datos más adecuadas.

Una vez llevadas a cabo las investigaciones mencionadas en los párrafos anteriores, la primera definición del mensaje NFFI [53], se llevó a cabo basándose en los trabajos realizados por el US Joint Blue Force Situation Awareness (JBFS) Advanced Concept Technology Demonstration (ACTD) [54], sobre la definición de un mensaje de seguimiento en formato XML. Los formatos de mensaje, que eran los más empleados por varios sistemas FTS americanos, fueron integrados de esta forma en único formato de mensaje, que se denominó JBFS.XML.

Se llevaron a cabo experimentos con mensajes con el formato JBFS.XML demostrando su buen funcionamiento, por esta razón se consideró que el formato de mensajes JBFS.XML facilitaba una buena aproximación de los datos reales manejados por los sistemas FTS. Los experimentos que se han mencionado anteriormente llevaron a la declaración de la versión 1.0 de la definición de mensajes NFFI.

En este punto, la NC3A llevó a cabo un análisis teniendo en cuenta otros estándares de modelado de datos internacionales de la OTAN, la intención de este análisis fue el hacer la primera definición de los mensajes NFFI más interoperable con sistemas FTS no estadounidenses.



Los principales estándares de modelado de datos, que se tuvieron en cuenta en el análisis llevado a cabo por la NC3A fueron los siguientes:

1). El Multilateral Interoperability Programme (MIP) Block-2 Data Model, Command and Control Information Exchange Data Model (C2IEDM). Este modelo de datos, que ha sido ampliamente analizado durante la presente tesis doctoral, es el modelo de datos más extendido entre la comunidad encargada de las operaciones terrestres dentro de la OTAN.

Por esta razón este modelo fue tomado como una referencia conceptual para la identificación y la nomenclatura de los datos que iban a componer formato del mensaje NFFI, así como para la definición del formato y los valores permitidos para estos datos.

La compatibilidad o al menos la posibilidad de mapear de una forma sencilla los datos contenidos en el formato de los mensajes NFFI con el modelo C2IEDM se consideró muy importante desde el principio, ya que era muy probable que datos contenidos en mensajes NFFI tuvieran que interactuar con sistemas de mando y control que usaran la solución MIP, es decir el C2IEDM, para implementar su interoperabilidad.

Los resultados del análisis llevado a cabo por la NC3A, permitieron que la versión 1.3 del formato de mensajes NFFI pudiera ser mapeada en una base de datos que contiene el C2IEDM con una pérdida mínima de elementos semánticas, que no afectaba a la integridad de los datos.

2). Un análisis del modelo Joint C3 Information Exchange Model (JC3IEDM) [29] fue también llevado a cabo, aunque este no alcanzó el nivel de detalle que alcanzo el análisis del C2IEDM, debido a la falta de madurez del modelo JC3IEDM a la hora de llevar a cabo el mencionado análisis, no obstante el programa NFFI continuará monitorizando las siguientes versiones del modelo desarrolladas por MIP para asegurar una futura compatibilidad NFFI-JC3IEDM.

3). El estándar NATO APP-6A (STANAG 2019) [55], también fue analizado por la NC3A. Este estándar es la evolución del US DOD MIL-STD 2525 [56], que es el estándar usado para definir la simbología de las unidades militares (incluyendo equipamientos e instalaciones).

Este estándar se consideró muy importante y aplicable a la actual caracterización de las unidades seguidas por los sistemas FTS, cuya representación de forma estandarizada en estos sistemas, se considera un aspecto muy relevante del análisis.

El APP-6A “Symbol ID Code” un carácter codificado con 15 dígitos ha sido escogido como estándar de caracterización de las unidades militares dentro del formato NFFI.

4). Para estandarizar de alguna forma los distintos códigos de caracteres usados por los distintos países se analizó el STANAG 1059 Edition 8 [57], “Character Codes for Geographical Entities” de 19 de febrero de 2004, siendo escogido como principal estándar de codificación de caracteres del formato NFFI.

Una vez descritos los orígenes del formato de mensajes NFFI para la interoperabilidad de sistemas FTS y enunciado los estándares que se han tenido en cuenta en su elaboración, se va a describir la estructura lógica de los mensajes de la versión 1.3 del NFFI.

La estructura lógica del formato de los mensajes de la versión 1.3 del NFFI está compuesta por cinco secciones principales, estas secciones son las siguientes:

- Sección de datos de posicionamiento (*positionalData*): Esta sección está compuesta por datos básicos de posicionamiento y identificación de seguimiento. Se compone de un conjunto de elementos que constituyen la mínima porción de datos que necesita ser intercambiado entre dos sistemas para caracterizar un seguimiento de una unidad. Esta sección es obligatoria en la definición del esquema del mensaje NFFI. El esquema de esta sección del mensaje NFFI se puede ver en la figura 42.

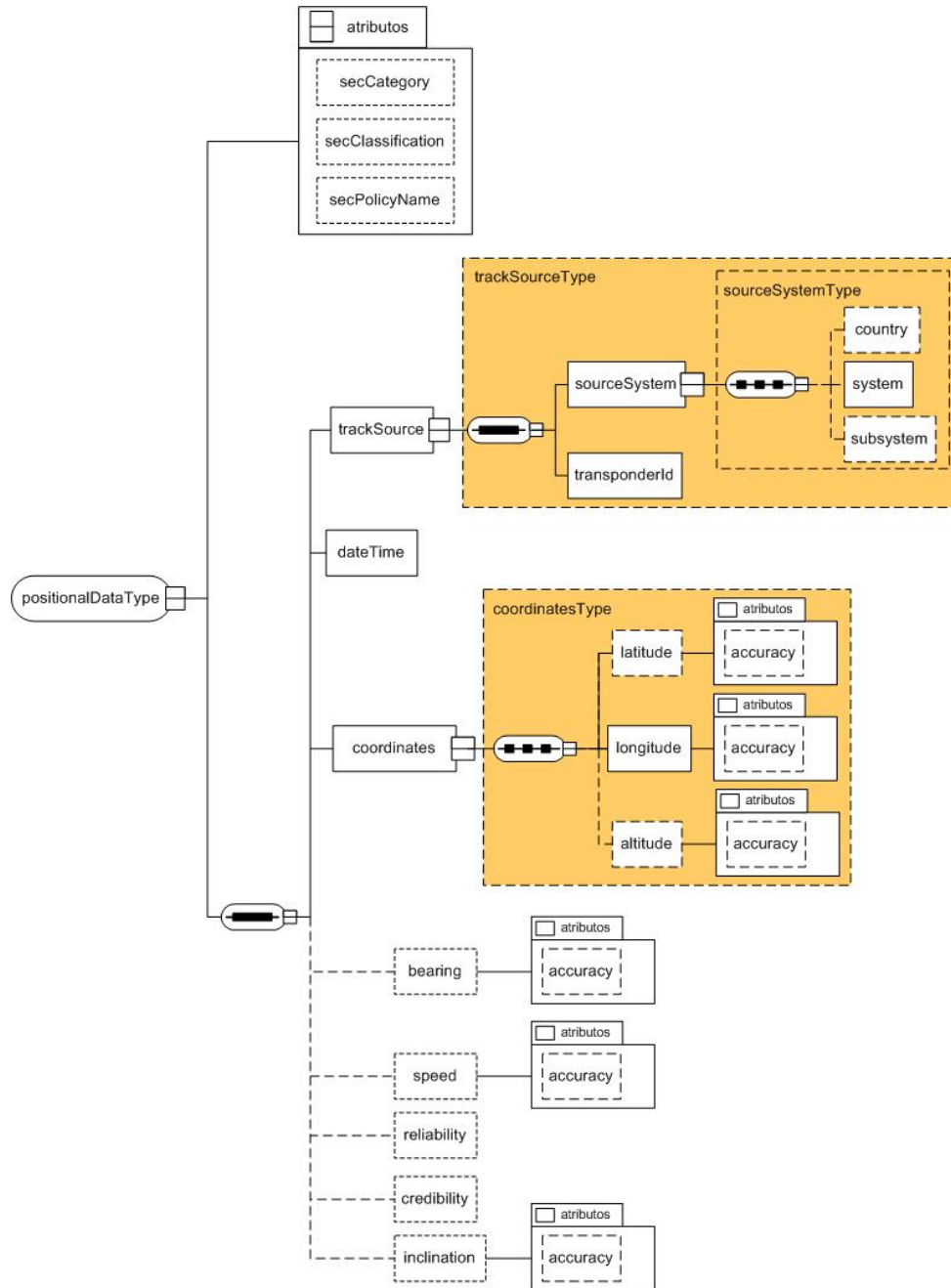


Figura 42

- Sección de datos de identificación (*identificationData*): Los elementos de esta sección están agrupados de forma que se facilita la identificación de la unidad que está asociada con la información de posicionamiento. Esta sección es opcional en la definición del esquema del mensaje NFFI. El esquema de esta sección del mensaje NFFI se puede ver en la figura 43.

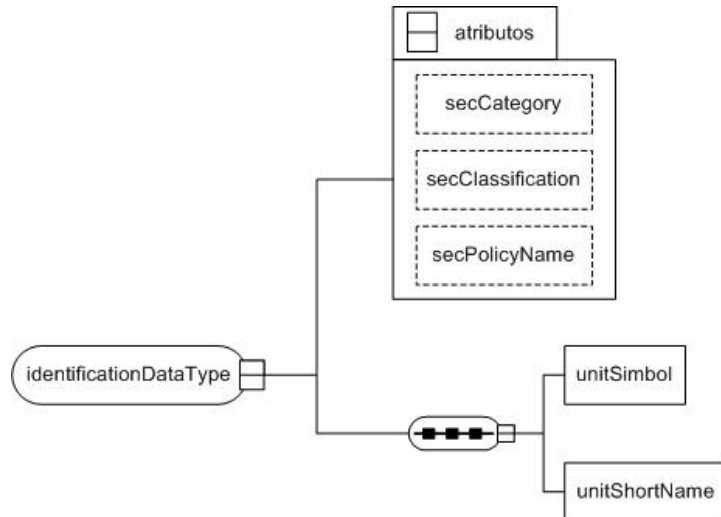


Figura 43

- Sección de estado operativo (*operStatusData*): esta sección facilita información sobre el estado operativo de la unidad relacionada con la sección de datos de posicionamiento. Todos los elementos de esta sección son opcionales. El esquema de esta sección del mensaje NFFI se puede ver en la figura 44.

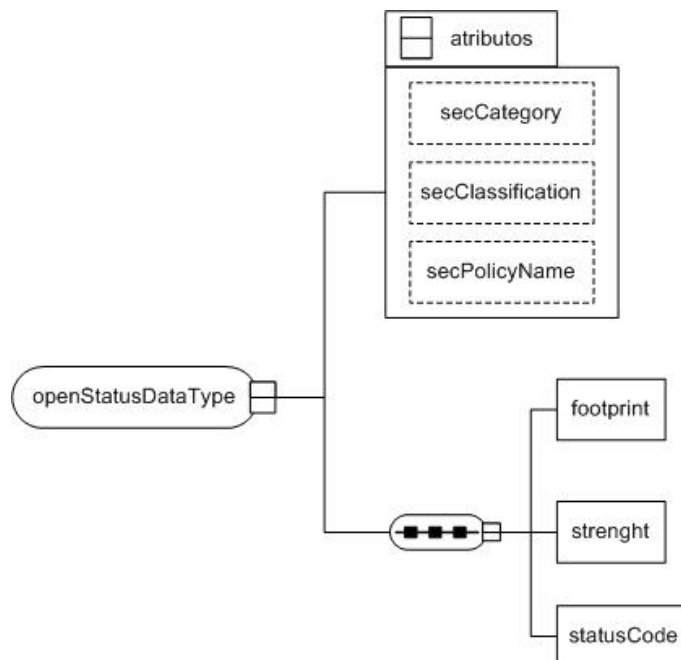


Figura 44

- Sección de datos específicos de sensores (*deviceSpecificData*): Esta sección facilita datos adicionales que pueden ser facilitados por sensores. Esta sección incluye datos que no todos los sistemas FTS pueden facilitar. Está sección es opcional en la definición del esquema del mensaje NFFI. El esquema de esta sección del mensaje NFFI se puede ver en la figura 45.

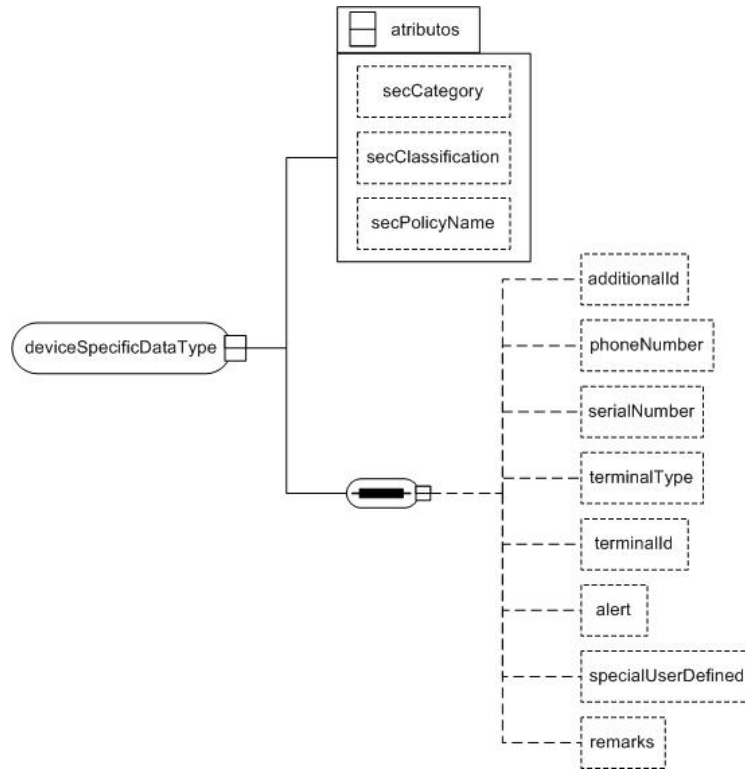


Figura 45

- Sección de datos detallados (*detailData*): Esta es una sección abierta por el momento y pensada para futuras informaciones muy específicas. Las definiciones de los esquemas o formatos de esta información específica está todavía bajo discusión. Está sección es opcional en la definición del esquema del mensaje NFFI. El esquema de esta sección del mensaje NFFI se puede ver en la figura 46.

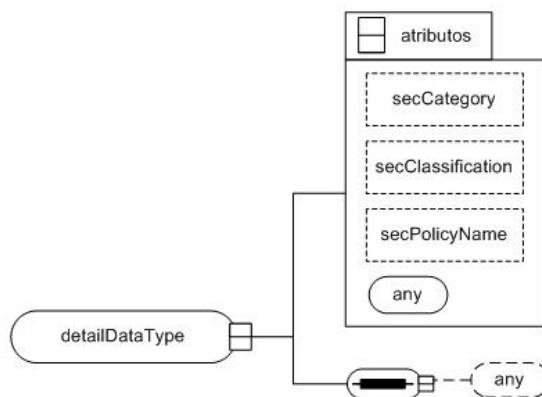


Figura 46

La estructura completa del mensaje NFFI versión 1.3 se puede ver en la figura 47.

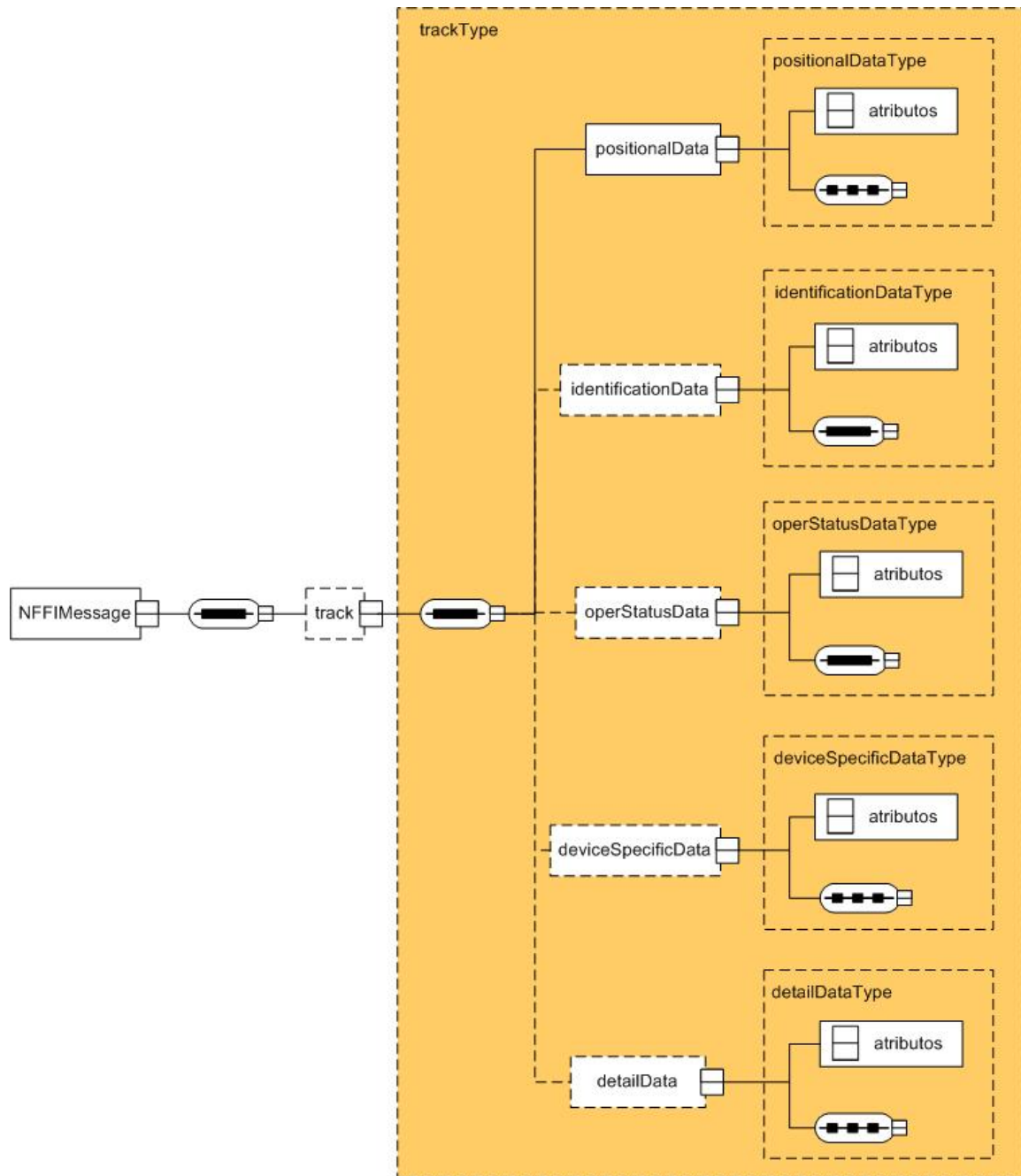


Figura 47

Un mensaje NFFI, o bien puede estar vacío o tiene que tener datos al menos en la sección de datos de posicionamiento de un elemento seguido. La cabecera XML estándar formara siempre parte del mensaje aun cuando se trate de un mensaje vacío.

De acuerdo con la definición NFFI los datos de posicionamiento es la única sección obligatoria en un proceso de seguimiento. Ninguna de las secciones opcionales puede ser transmitida sin los datos de la sección de posicionamiento.

Por lo tanto es obligatorio que todas las aplicaciones NFFI soporten al menos el procesado del formato de la sección de datos de posicionamiento del mensaje NFFI. El hecho de que soporten o no el procesado de las secciones opcionales del mensaje NFFI no es obligatorio.

Si existe información opcional en el mensaje NFFI y no existe capacidad de proceso para las secciones opcionales en la aplicación receptora, el mensaje puede ser aceptado y esta información ignorada.

El elemento “tracSource” de la sección de datos de posicionamiento contiene datos que son una combinación de los datos del dispositivo que transmite los datos y el sistema que recoge estos datos. El valor de este elemento ha de ser único para cada pareja dispositivo-sistema para de esta forma identificar de una forma inequívoca la fuente de la información.

Un proceso de seguimiento puede ser inequívocamente identificado por los valores de los elementos “tracSource” y “dateTime” de la sección de datos de posicionamiento.

A continuación se describirá el proceso recomendado por el estándar NFFI v1.3 para el mapeo de datos con el modelo de datos C2IEDM, ya que este proceso será utilizado en la aplicación de réplica NFFI, que ha sido implementada como parte de la presente tesis, para el mapeo de los datos de los mensajes NFFI en el interfaz de datos del sistema FPTS propuesto, que esta basado en el modelo C2IEDM v6.15c.

El mapeado de los datos en este caso consiste en transformar el contenido del mensaje NFFI en otro formato, teniendo en cuenta la relación de correspondencia entre la definición del mensaje NFFI y las definiciones relevantes de otros formatos.

En el estándar NFFI se ha tenido en cuenta la posibilidad de mapear a/desde el modelo C2IEDM, para asegurar que los datos de seguimiento NFFI, son compatibles y pueden ser traducidos a/desde el modelo C2IEDM sin pérdidas semánticas significativas.

Un seguimiento (track) se usa en la especificación NFFI para identificar un objeto móvil, en particular un objeto móvil terrestre. En términos del modelo C2IEDM el seguimiento NFFI representa el aspecto funcional del objeto no el objeto físico en si mismo. El concepto caracterizado como un seguimiento (track) en el modelo C2IEDM se ve como un objeto (instancia) OBJECT-ITEM de la categoría ORGANISATION y de la subcategoría UNIT. Cada seguimiento (instancia de OBJECTÍTEM) requiere un objeto OBJECT-TYPE, el cual es mapeado o bien desde el elemento “unitSymbol” del mensaje NFFI o si el elemento “identificationData” no existe en el mensaje, se mapea como un seguimiento (track) genérico (objeto OBJECT-TYPE).

El identificador del seguimiento del mensaje NFFI (“transponderId”) se mapea dentro del atributo *objetc-item-name* y el campo “unitShortName” (si existe), se mapea dentro del atributo *unit-formal-abbreviated-name*. Si se dispone del campo “additionalId” en la sección “deviceSpecificData” del mensaje NFFI, este se mapea dentro del atributo *object-item-alternate-identification-text*.

La información de posición (latitud, longitud y altura) se mapea dentro del concepto LOCATION del C2IEDM y se enlaza con el seguimiento (instancia de OBJECTÍTEM) a través de la entidad OBJECT-ITEM-LOCATION la cual también cubre información relativa a ángulos y velocidad.

El país al cual pertenece una unidad se extrae del valor del campo “unitSymbol” (de acuerdo con la especificación APP-6A) y es mapeado dentro de la entidad AFFILIATION y es asociado con el seguimiento (instancia de OBJECTÍTEM) a través de la entidad OBJECT-ÍTEM-AFFILIATION.

El estado operacional de la unidad y los datos específicos del dispositivo sensor, definidos en las secciones del mensaje NFFI “operStatusData” y “deviceSpecificData” respectivamente, son mapeados en sus correspondientes estructuras dentro del C2IEDM, por ejemplo, el campo NFFI “phoneNumber” se mapea en el atributo *electronic-address-name*, el campo NFFI “serialNumber” se mapea en el atributo *material-serialnumber-identification-text*, el campo NFFI “strength” se mapea en el atributo *holding-total-quantity*, etc.

Muchos de estos datos específicos del dispositivo requieren un complejo conjunto de estructuras de datos dentro del C2IEDM para asociar la información con el seguimiento básico (instancia de OBJECT-ITEM).

Cada asociación individual dentro del C2IEDM incluyendo OBJECT-ITEM-TYPE, OBJECT-ITEM- LOCATION y OBJECT-ITEM-AFFILIATION requieren una instancia de la entidad REPORTING-DATA separada. Los detalles básicos para estas entradas en la tabla REPORTIG-DATA se derivan de la sección “positionalData” del mensaje NFFI en particular de los campos “dateTime” para los valores de los atributos *effective-date/time* y “sourceSystem” para el atributo *reporting-organisation*.

También se tiene en cuenta en la especificación del mapeo de datos con el modelo C2IEDM que se especifica en el estándar NFFI, que el C2IEDM es un modelo complejo y normalizado y que cada inserción de datos en su estructura requiere un número de datos adicional para mantener la integridad de atributos y relaciones.

En conclusión la información facilitada por los mensajes NFFI, puede ser mapeada sin muchos problemas dentro del modelo de datos C2IEDM de MIP. Los formatos de los campos del mensaje NFFI son prácticamente iguales a sus correspondientes atributos dentro del C2IEDM, las excepciones son básicamente campos con formato de texto libre, como el campo “remarks” y los campos genéricos del mensaje NFFI “specialUserDefined” y “detailData”.

También se debe aclarar que existen campos del mensaje NFFI que presentan más complejidad que otros a la hora de mapear su información dentro del modelo C2IEDM, por ejemplo, algunos campos de la sección “deviceSpecificData” del mensaje NFFI, como es el caso de los campos “phoneNumber”, “serialNumber” y “terminalType”/“terminalId”.

Además de lo expuesto anteriormente sobre el mapeado de la información de los mensajes NFFI dentro del modelo C2IEDM, existe una importante consideración que hay que tener en cuenta a la hora de mapear datos NFFI dentro del modelo C2IEDM.

Esta consideración es la siguiente; no existe correspondencia directa entre identificadores, por ejemplo el atributo *object-item-id*, que indicaría el identificador del objeto seguido, no tiene su correspondiente campo en el mensaje NFFI.

Por lo tanto el mapeado de esta información se debe basar en búsquedas asociativas concatenando elementos del mensaje NFFI como pueden ser “unitShortName” y “unitSymbol” que pueden ser usados como claves secundarias en el modelo C2IEDM. Los valores de los identificadores NFFI para identificar una unidad seguida (“positionalData.trackSource”, i.e. “sourceSystem” y “transponderId”) no tienen correspondencia directa con claves primarias del modelo C2IEDM para unidades (UNIT), es decir no se corresponden directamente con un atributo object-item-id.



### **3.5.1.5 Implementación del uso del formato de mensajes NFFI**

Como parte de los desarrollos sobre interoperabilidad entre sistemas C2IS llevados a cabo en la presente tesis doctoral, se ha implementado una aplicación de réplica de datos que utiliza la definición del estándar NFFI v1.3 [51], para facilitar la interoperabilidad entre sistemas FFTS (Friendly Force Tracking System).

Esta aplicación será integrada en el sistema, que se va a proponer en la presente tesis, como sistema FFTS para ser usado por los distintos cuerpos y servicios de seguridad, que actúen de forma conjunta en la resolución de una crisis civil.

La aplicación desarrollada permitirá la interoperabilidad del sistema FFTS propuesto en el plano horizontal, es decir, entre los distintos nodos de primer nivel de los distintos sistemas FFTS, que participen en la resolución de la crisis.

Será en estos nodos donde se procesa tanto el posicionamiento, como el resto de la información que envían las unidades desplegadas sobre el terreno.

De esta forma, cuando el sistema propuesto tenga integrada esta aplicación de réplica, utilizará por un lado el estándar NFFI v.1.3 para facilitar la interoperabilidad con los nodos FFTS encargados del seguimiento de las unidades pertenecientes a las distintas entidades participantes en la gestión de la crisis y por otro lado, se utilizará la aplicación de réplica que implementa el estándar MIP, cuya descripción se puede ver en apartados anteriores, para la réplica de información en el plano vertical, es decir entre los nodos de distinto nivel jerárquico pertenecientes a la misma entidad.

La aplicación de réplica que basada en el estándar NFFI v1.3 ha sido implementada a finales de 2006 y será probada durante las pruebas de interoperabilidad del programa CWID 2007 [58], que se realizarán en Jørstadmoen (Noruega) en junio de 2007. El resultado de estas pruebas será ampliamente descrito en apartados posteriores de la presente tesis.

El modo de funcionamiento, en lo referente a la réplica de datos, del sistema propuesto por esta tesis como solución de mando y control en gestión de crisis civiles y que se acaba de describir en los párrafos anteriores, es el que se describe en la figura 48

En esta figura se puede ver como los nodos de los sistemas FFTS de las distintas entidades que participan en la resolución de la crisis, (bomberos, servicios sanitarios y ejército) interoperan entre si utilizando el estándar NFFI, replicando las posiciones de sus unidades a los demás nodos FFTS en el plano horizontal.

Por otro lado, se puede ver también en la figura 48 el plano vertical de réplica de la información del servicio de bomberos, los demás planos verticales de réplica de datos correspondientes a los servicios sanitarios y al ejército, tendrían la misma estructura, pero no han sido incluidos en la figura por razones de espacio.

En este plano vertical se puede ver como los distintos nodos FFTS replican las posiciones de sus unidades desplegadas sobre el terreno, al nodo de mando y control de primer nivel utilizando el estándar MIP para interoperabilidad de sistemas C2I.

A su vez, los nodos de mando y control de primer nivel replicarán sus datos al nodo de mando y control de segundo nivel, donde los responsables del cuerpo de bomberos en este caso tomarán las decisiones correspondientes, completando de esta forma la estructura jerárquica de mando y control del sistema.

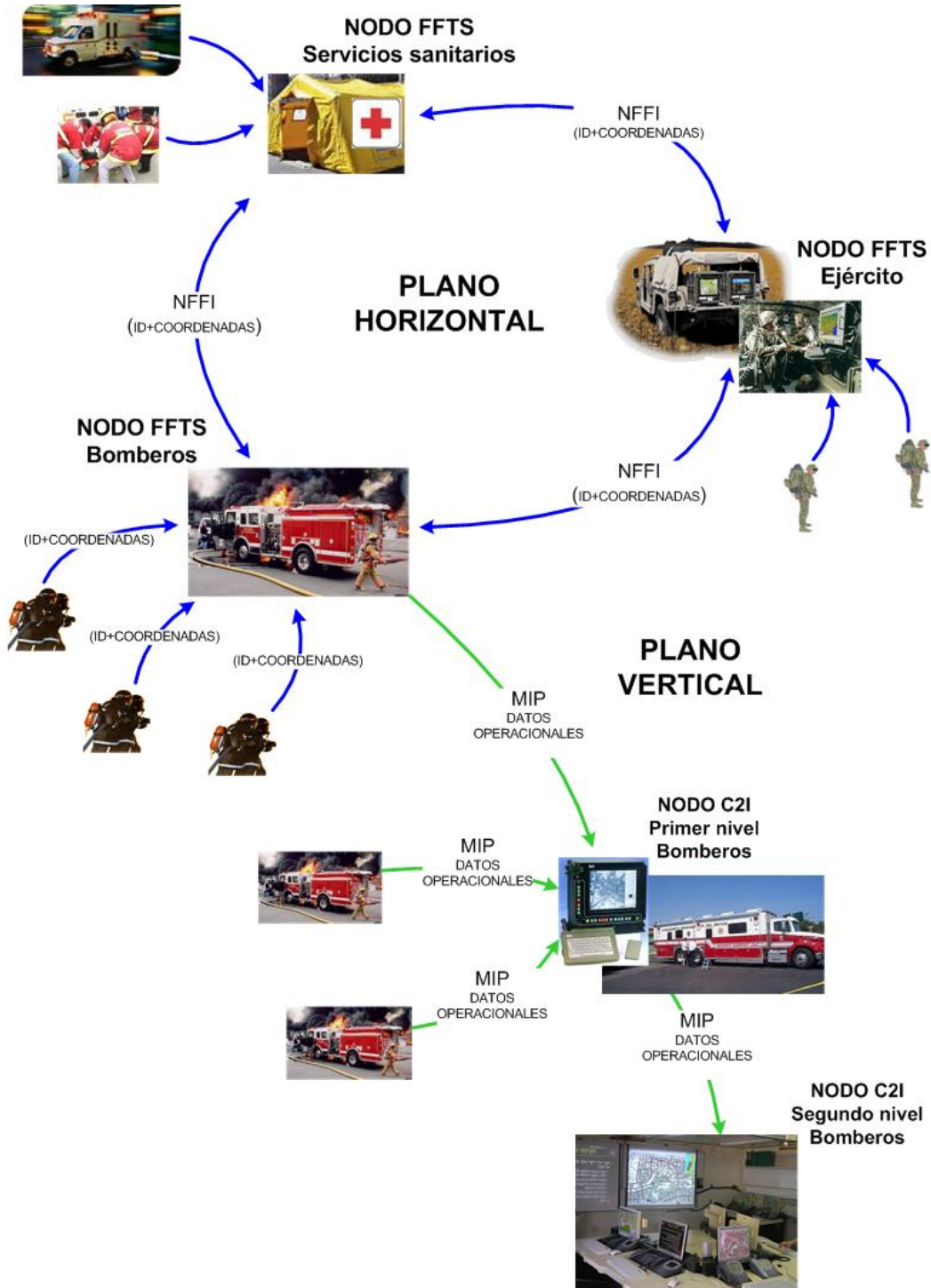


Figura 48

En los siguiente párrafos se realizará una descripción técnica de la aplicación de réplica basada en el estándar NFFI v1.3, que ha sido desarrollada en la presente tesis.

Los datos que se reciben desde las unidades desplegadas sobre el terreno vía WIFI se almacenan en el interfaz común de la base de datos del sistema, este interfaz de datos es compatible con el estándar MIP de réplica de datos.

La aplicación de réplica NFFI mapea los datos de posicionamiento de las fuerzas propias almacenados en el interfaz de datos basado en el modelo C2IEDM, a una base de datos intermedia específicamente diseñada para contener datos compatibles con el estándar NFFI, a partir de estos datos copiados en esta base de datos se compondrá el mensaje NFFI, que se enviará a los demás sistemas FFTS de la red.

La aplicación de réplica implementada compone el mensaje NFFI con los datos recibidos. Con los datos de posicionamiento y el identificador de cada unidad rellena las secciones de posición de la unidad (positionalData) y identificación de la unidad (identificationData).

Las secciones de información sobre el estado de la unidad (operStatusData), la de información específica de dispositivo (deviceSpecificData) y la de detalles (detailData) se dejan en blanco.

En cuanto a la recepción de datos el sistema actúa de la siguiente forma, recoge los mensajes NFFI que le llegan de los demás sistemas FFTS de la red y almacena esta información en la base de datos intermedia, una vez realizado este paso la aplicación mapea estos datos en el interfaz común de datos MIP siguiendo las normas de mapeo de datos con el modelo C2IEDM descritas en el estándar NFFI.

De esta forma el sistema puede visualizar las posiciones de las fuerzas amigas recibidas por pantalla, obteniendo de esta forma una visión común del espacio de operaciones.

La descripción de la base de datos intermedia es la siguiente;

Esta base de datos intermedia esta compuesta por cinco entidades independientes entre si, representadas por las siguientes tablas: pos\_data, id\_data, op\_stat\_data, dev\_spec\_data y detail\_data.

Cada tabla representa una sección del mensaje NFFI, incluyendo un atributo en la tabla por cada campo de la sección del mensaje NFFI a la que representa.

Cuando un mensaje NFFI es recibido por la aplicación de réplica de datos, se introduce en cada una de las tablas de la base datos intermedia, la información asociada a la sección del mensaje NFFI a la que representa cada tabla.

Cada tupla de cada tabla correspondiente con un mismo mensaje NFFI queda identificada con el mismo número de secuencia.

Una vez se ha recibido el mensaje NFFI y la información de cada uno de sus campos ha sido almacenada en su tabla correspondiente, se procede por parte de la aplicación de réplica, al mapeo de estos datos recibidos dentro del interfaz de datos del sistema FFTS siguiendo las recomendaciones de mapeo de datos NFFI con el modelo C2IEDM que especifica el estándar NFFI, ya que el interfaz de datos del sistema FFTS propuesto, esta basado en el modelo de datos C2IEDM v6.15c.

Cabe destacar en este punto que la aplicación de réplica tiene en cuenta a la hora de mapear los datos de los mensajes NFFI los posibles problemas de integridad de datos que pudiera tener el interfaz de datos basados en el modelo C2IEDM.

La descripción del esquema físico de la base de datos intermedia en la que se almacenan los datos de las secciones de los mensajes NFFI recibidos se puede ver en la figura 49.

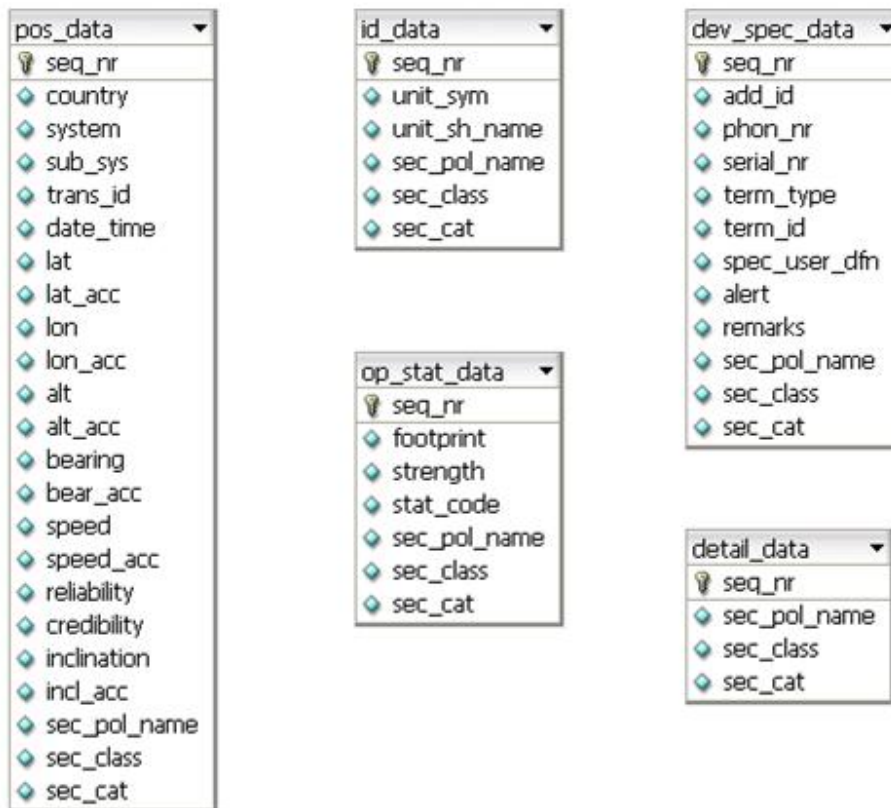


Figura 49

Otro aspecto importante de la aplicación de réplica desarrollada es la frecuencia de la réplica de las posiciones, esta funcionalidad se consideró variable y dependiente de los parámetros y las características de cada operación, por lo tanto esta funcionalidad es ajustable y se acuerda de antemano con los distintos sistemas FFTS participantes en cada operación.

No se puede considerar de igual forma la réplica de posiciones que se llevaría a cabo en una operación donde no se espera mucha variación de las posiciones de las fuerzas amigas, como podría ser un despliegue acorazado en entorno urbano, donde cada carro cubre un cruce de calles y permanece en él hasta el final de la operación, que la réplica de datos de posiciones de una operación de avance rápido de vehículos ligeros, donde las posiciones de las unidades cambian constantemente y es necesarios tener un exhaustivo seguimiento de las mismas.

Para una operación del primer tipo descrito se realizaría una réplica de datos cada vez que se recibiera una nueva posición por parte de la unidad.

Para una operación como la descrita en segundo lugar, se realizaría una réplica de datos de posición cada cierto tiempo, por ejemplo un minuto, ya que de otra manera, la continua llegada de nuevas posiciones de las distintas unidades podría congestionar tanto la red como el sistema.

En lo que se refiere al protocolo que utiliza la aplicación de réplica NFFI se ha seguido escrupulosamente la descripción del protocolo NFFI que se hace en su documento de especificaciones.

La descripción completa del proceso de réplica de datos utilizando el estándar NFFI se puede ver en la figura 50.

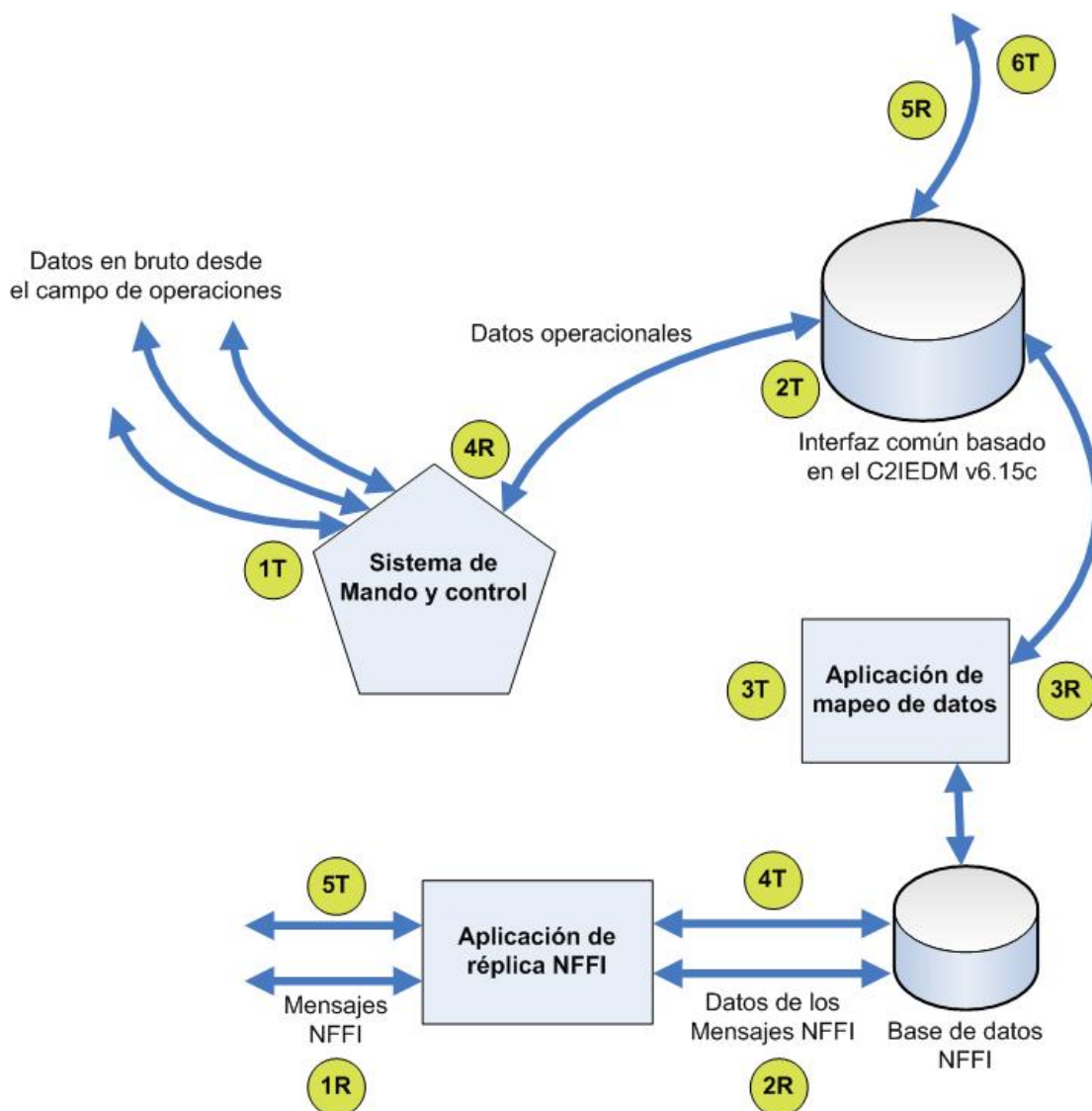


Figura 50

En esta figura podemos ver como actúa el sistema tanto en transmisión como en recepción, en transmisión se puede ver que las posiciones de las fuerzas propias llegan al sistema FFTS desde el espacio de operaciones (Ver número 1T en figura 50) y este las almacena en su interfaz de datos (Ver número 2T en figura 50).

Una vez almacenados en el interfaz de datos la aplicación de réplica mapea estos datos en la base de datos intermedia (Ver número 3T en figura 50) para a continuación componer el mensaje NFFI (Ver número 4T en figura 50) y enviarlo los demás sistemas FFTS (Ver número 5T en figura 50). A la vez que el sistema FFTS propuesto envía las posiciones de las fuerzas propias a los demás sistemas FFTS, este réplica estas posiciones a su nodo de mando y control de orden superior (Ver número 6T en figura 50).

En recepción el sistema actuaría a la inversa, recibiría los mensajes NFFI de los demás sistemas FFTS (Ver número 1R en figura 50), almacenaría su contenido en la base datos intermedia (Ver número 2R en figura 50) y posteriormente mapearía estos datos dentro del interfaz de datos del sistema FFTS (Ver número 3R en figura 50). Finalmente el sistema FFTS visualizaría las posiciones recibidas (Ver número 4R en figura 50) y las transmitiría al nodo de mando y control de nivel superior (Ver número 5R en figura 50).







## **4 Validación de un modelo de datos táctico para la gestión de emergencias**

### **4.1 Introducción**

En este capítulo se va describir en detalle tanto el sistema SIMACOP, en el que se ha integrado el modelo de datos propuesto por la presente tesis, como las pruebas oficiales de interoperabilidad del programa CWID 2007 en las que ha participado SIMACOP y cuyos resultados, como se verá en los siguientes apartados, validan el modelo de datos diseñado e implementado en la presente tesis doctoral.

### **4.2 Descripción del sistema SIMACOP**

El sistema SIMACOP (SIstema de MAndo y COntrol para Pequeñas unidades) es el fruto del proyecto de investigación; TIN2004-03588-C4ISR Multimedia aplicado a la gestión de emergencias, financiado por el Ministerio de ciencia y tecnología y fondos FEDER. Una gran parte de la investigación desarrollada en la presente tesis doctoral se realizó durante el desarrollo de este proyecto.

En el proyecto se propone la migración y adaptación de los conceptos operativos y tecnológicos desarrollados en los sistemas C4ISR militares, plasmados en el estándar del DoD (Department of Defence) de Estados Unidos [59], al campo civil.

En particular, en el proyecto se propone una adaptación de estos sistemas a la gestión de emergencias por su elevado impacto social (incendios, inundaciones, atentados terroristas, vertidos tóxicos, etc.), con la innovación tecnológica de la inclusión masiva de flujos multimedia (streaming) en todos los niveles de comunicación y procesamiento del sistema C4ISR, aspecto innovador respecto a los sistemas militares dados los condicionantes operativos de los mismos.

Por otra parte, los sistemas C4ISR son eminentemente distribuidos y predecibles [60] al tratarse de sistemas eminentemente dinámicos, por lo que el desarrollo de aplicaciones concretas a partir componentes middleware genéricos, minimiza los costes de desarrollo y permite la portabilidad e interoperabilidad frente a los tradicionales sistemas empotrados.

Los sistemas de mando y control son uno de los ejemplos clásicos de sistemas de tiempo real críticos (hard real time). Las siglas que han ido identificando a este tipo de sistemas con el paso del tiempo (C2I, C3I, C4I), han ido reflejando la incorporación de funciones a los mismos, en concordancia al avance de las tecnologías de computación y comunicaciones.

Los más avanzados sistemas de mando y control actuales se denominan C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) [61]. Los sistemas C4ISR, y en general todos los sistemas de mando y control, se definieron en ámbito tecnológico militar, y han demostrado su eficacia en la reciente Guerra de Irak [62].

Algunos intentos de trasladar la arquitectura de estos sistemas al plano civil, y en especial su modelo de datos, se pueden encontrar en la bibliografía [63].

En este sentido se ha de destacar que un aspecto fundamental de un sistema C4ISR es la capacidad de interoperar con otros sistemas C4ISR, es decir, poder compartir información en tiempo real con otros nodos C4ISR, por ejemplo, el sistema de mando y control del Ejército de Tierra con el de la Fuerza Aérea o la Armada.

Por ello desde el DoD y la NATO se han emitido varios estándares o marcos de trabajo que incluyen la metodología para la definición de arquitecturas de sistemas C4ISR, que permitan posteriormente la interoperabilidad de sistemas distintos, siempre que sigan el mismo marco de trabajo [61] [64].

Existen evidentes similitudes operativas entre las necesidades de gestión de unas fuerzas militares en un escenario de combate y la gestión de unas fuerzas civiles (bomberos, policía, equipos sanitarios) en una emergencia producida por un desastre natural (incendio foresta, inundación, huracán), un accidente (de tráfico, hundimiento de un barco, caída de un avión) o un atentado terrorista, sin pretender ser exhaustivos.

Algunas propuestas de aplicación de sistemas de mando y control a este tipo de eventos se pueden encontrar en la bibliografía [65].

Por las razones anteriormente expuestas, se considera que la aplicación directa de las metodologías de diseño de sistemas C4ISR de DoD, así como una estructura de datos orientada a la interoperabilidad de sistemas, a un sistema civil de gestión de emergencias es una aportación totalmente novedosa.

Es evidente, que el sistema de gestión de emergencias, será dependiente de la propia naturaleza de la emergencia. No es lo mismo una inundación (el agua es un enemigo/objetivo amplio, indefinido, semejante a un arma de destrucción masiva) que un incendio (que se trata de un enemigo/objetivo mucho más definido).

Por ello en el proyecto, se planteará una arquitectura genérica, siguiendo la filosofía del DoD y de la NATO, que puede ser la base de distintos sistemas concretos (para uso de bomberos, policía, protección civil, sanidad, etc.), y precisamente por su carácter genérico permitir su interoperabilidad en el caso de una emergencia común.

La recomendación IEEE STD 610.12 [66], define arquitectura de un sistema como: “La estructura de componentes, sus relaciones, y los principios y líneas maestras que rigen su diseño y evolución en el tiempo”.

Según el Modelo de Referencia del DoD la arquitectura de sistemas C4ISR estará compuesta por 3 planos, 1) operativo: descripción de las tareas y actividades de los elementos operativos del sistema, así como del flujo de información entre los mismos, 2) sistemas: descripción de los sistemas físicos y lógicos, así como de sus interconexiones, 3) tecnológico: componentes y estándares involucrados en la implementación del sistema.

La definición de una arquitectura consiste en generar una serie de productos para cada plano que lo describen inequívocamente.

La estructura de planos propuesta por el DoD se puede ver en la figura 51.



**Figura 51**

Por otra parte, los sistemas de mando y control, tradicionalmente se han diseñado e implementado, como sistemas empotrados [67], lo que implica tres grandes penalizaciones: elevados costes de desarrollo, escasa interoperabilidad con otros sistemas, difícil escalabilidad y mantenimiento.

Sin embargo, los avances que la tecnología civil ha experimentado en el campo TIC durante los últimos años, permite el diseño e implementación de sistemas de tiempo real distribuidos, incluso en el ámbito militar, según el principio COTS (Commercial- of- the-self) [68].

En los sistemas COTS se reducen los costes del sistema por dos razones;

- 1) Se utiliza hardware con especificaciones civiles siempre que el entorno de funcionamiento lo permita.
- 2) Las aplicaciones se implementan a partir de objetos genéricos, reutilizables, implementados en lenguajes de programación de alto nivel (C, C++, Ada, e incluso Java).

Por supuesto, si se pretende implementar un sistema de mando y control C4ISR para aplicaciones civiles, debe basarse en el principio COTS, aunque teniendo en cuenta que sólo un buen diseño y correcta implementación garantizarán las prestaciones de tiempo real del sistema [69] y por tanto su utilidad.

En lo referente a las comunicaciones el objetivo de los sistemas C4ISR interoperables requiere transmisión de información actualizada, información en todos los sentidos, desde y hacia los centros de coordinación a diferentes niveles y los puntos de actuación (flujo de información vertical), así como entre las diferentes organizaciones (flujo de información horizontal). Esto supondrá comunicaciones robustas, eficientes y coordinadas en tiempo real, inter e intra organizaciones.

La tendencia actual en la distribución de información y control en los sistemas C4ISR se dirige a la utilización de medios de comunicación transparentes y robustos para el usuario.

Las redes de comunicaciones empleadas deben ser digitales con carácter civil y/o militar, permitiendo en el futuro la incorporación de información multimedia.

La arquitectura de comunicaciones en los sistemas C4ISR, ya sea para su uso militar o civil [70], se estructura, como puede apreciarse en la figura 54, en varios niveles de jerarquía a nivel de red [65] [71]. Estos niveles jerárquicos a nivel de red son los que se van a describir a continuación:

- **Personal Area Network (PAN)**, se encargará de conectar los sensores que porten unidos a su cuerpo los operadores (i.e. soldados, bomberos,...). Este tipo de sensores se comunicará mediante WLAN o BlueTooth. [72] [73]
- **Red de combate o de campo**, conecta al personal que está operando en la zona de actuación entre ellos (i.e. soldados de una unidad de combate o bomberos en tareas de extinción de un incendio) y a su vez con el primer nivel mando, que se encuentra junto a los operativos en zona de actuación. Se utiliza fundamentalmente tecnología inalámbrica, fundamentalmente WLAN. [74]
- **Red táctica**, conecta al personal de primer nivel de mando con los mandos de las diferentes unidades operativas, para que estos transmitan la información destinada a cada uno de los individuos en la zona de actuación a través de la red de combate o de campo. Se emplea tecnología inalámbrica WLAN, redes móviles comerciales o comunicaciones vía satélite, dependiendo de la cobertura y despliegue de las unidades operativas. [75]
- **Red estratégica**, conecta el centro de coordinación de una determinada organización con los mandos del primer nivel. Se utiliza fundamentalmente enlaces satélite o de fibra óptica. En el caso de existir varias redes estratégicas debería existir flujo de información entre los centros de coordinación de nivel superior, por lo que se podría plantear la existencia de una red estratégica de coordinación global.

Tanto la arquitectura de red como las redes diferentes que la componen pueden verse en la figura 52.

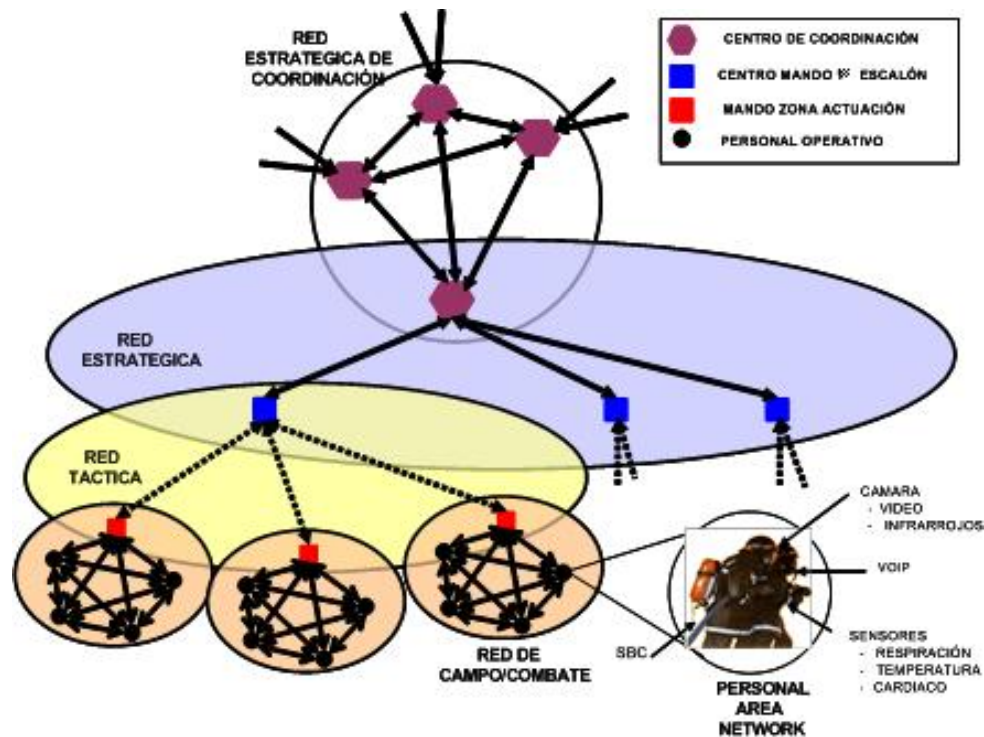


Figura 52

La arquitectura de comunicaciones debe cumplir las siguientes características: 1) tolerancia a fallos, 2) incorporar protocolos de tiempo real, 3) movilidad en la red de campo/combate, 4) interoperabilidad en la red táctica, 5) cobertura global en la red estratégica y 6) suficiente ancho de banda para el tipo de información de mando y control intercambiado. [65] [76]

Las tecnologías disponibles para la comunicación en sistemas C4ISR son: redes de radio terrestres de tipo trunking (recomendadas para el sector de seguridad público europeo); redes de comunicación de satélite; tecnología WLAN (i.e. IEEE 802.11 a/b/g), para la interconexión de sensores y el establecimiento de redes “ad hoc”; Bluetooth para la conexión de sensores según el concepto de wearable computers [77]; terminales robustos (i.e. Single Board Computers, SBC); enlaces de fibra óptica pertenecientes a las organizaciones o alquilados a operadores de comunicaciones; protocolos de comunicaciones de tiempo real; redes móviles del tipo UMTS o GPRS.

Áreas clave de investigación del proyecto en el campo de las comunicaciones aplicables a los sistemas C4ISR incluyen: vídeo avanzado y de calidad; técnicas mejoradas de compresión de datos para la transmisión de volúmenes de datos crecientes sobre canales de ancho de banda limitado y utilización de redes inalámbricas de área local (WLAN) o de área mediante estaciones base; redes de fibra óptica para proporcionar conectividad robusta, de bajo coste y con gran ancho de banda a las comunicaciones terrestres.

### 4.3 Diseño del núcleo común de un modelo de datos para emergencias civiles e implementación del mismo en el sistema SIMACOP

Una vez descritas las características más importantes de las comunicaciones y de la arquitectura del sistema propuesto en el proyecto TIN2004-03588-“C4ISR Multimedia aplicado a la gestión de emergencias”, vamos a pasar a describir la estructura de datos diseñada para este sistema, dentro de la investigación desarrollada en la presente tesis doctoral, la cual está basada en un modelo de datos con un núcleo común, que permitirá su interoperabilidad con otros centros de coordinación que implementen la misma solución.

Tras el estudio detallado de las principales versiones de todos los modelos de datos tácticos desarrollados dentro de los programas ATTCIS y MIP realizado en los primeros capítulos de esta tesis doctoral, se ha escogido una solución de modelo de datos táctico con núcleo común, para ser implementada como modelo de datos del sistema SIMACOP.

Se ha elegido esta solución con la intención de permitir la interoperabilidad de los distintos nodos de SIMACOP desplegados durante las pruebas del sistema, por otra parte se ha de destacar que el núcleo común del modelo de datos de SIMACOP se ha basado en el modelo C2IEDM v6.15c, lo cual facilitará su integración e interoperabilidad con sistemas de mando y control reales cuyo modelo de datos este basado en la solución MIP, un ejemplo podría ser el Sistema de Mando y Control del Ejército de Tierra (SIMACET) [78].

SIMACOP es en si mismo, por su diseño conceptual, un sistema de seguimiento de fuerzas amigas o Friendly Force Traking (FFT) system, si utilizamos la terminología anglosajona, el cual es aplicable tanto a entornos civiles como militares. Al tratarse de un sistema FFT no necesita todas las funcionalidades, en lo que respecta a su modelo de datos, que necesitaría un sistema C4IRS. Por esta razón para diseñar el núcleo común del modelo de datos del sistema SIMACOP se han seleccionado una serie de tablas del modelo C2IEDM v6.15c con las que se cubren completamente los requerimientos del sistema.

En la tabla 9 se van a describir las tablas utilizadas para formar el núcleo común del modelo de datos de SIMACOP, especificando los atributos utilizados en cada tabla y los valores de los mismos utilizados durante las pruebas de campo del sistema.

Tabla	Atributos	Descripción
LOCATION	location_id	Identificador de la posición
	category_code	Tipo de posición. El valor utilizado es 'PT' (POINT)
OBJECT-ITEM-LOCATION	location_id	Identificador de la posición
	object_item_id	Identificador del object_item localizado
	obj_item_loc_ix	Siempre a 1 durante las pruebas
	acc_qty	Siempre a NULL durante las pruebas
	brng_angle	Siempre a NULL durante las pruebas
	brng_acc_angle	Siempre a NULL durante las pruebas
	speed_rate	Siempre a NULL durante las pruebas
	speed_acc_rate	Siempre a NULL durante las pruebas

	use_cat_code	Siempre a NULL durante las pruebas
	rptd_id	Fijado a '102' durante las pruebas
OBJECT-ITEM	object_item_id	Identificador del object_item localizado
	cat_code	El valor utilizado es 'PS' (PERSON)
	name	String vacio durante las pruebas
	altn_identific_txt	Siempre a NULL durante las pruebas
POINT	point_id	Identificador del punto
	cat_code	El valor utilizado es 'ABS' (ABSOLUTE)
ABSOLUTE-POINT	abs_point_id	Identificador del punto
	lat_coord	latitud en proyección WGS84
	long_coord	longitud en proyección WGS84
	angular_precision_code	El valor utilizado es 'THOUMN' Thousandth of minute (Aprox 2m)
	abs_point_ver_dist_id	Fijado a '11002' durante las pruebas
VERTICAL DISTANCE	ver_dist_id	Identificador de la distancia vertical
	cat_code	El valor utilizado es 'ALTUDE' (ALTITUDE)
	dim	Número de metros
	precision_code	Fijado a '10M' durante las pruebas
RPDT	rptd_id	Identificador del reporte de datos Fijado a '102' durante las pruebas
	acc_code	Fijado a '1' durante las pruebas
	cat_code	El valor utilizado es 'ASS' (Assumed)
	cntg_ind_code	Fijado a 'NO' durante las pruebas
	credibility_code	El valor utilizado es 'IND' (Indeterminate)
	reliability_code	El valor utilizado es 'A' (Completely reliable)
	rep_date	String vacio durante las pruebas
	rep_time	String vacio durante las pruebas
	source_type_code	El valor utilizado es 'POW' (Prisoner of War)
	timing_cat_code	El valor utilizado es 'TIMNA' (Timing not available)
	ref_id	Identificador de la referencia
	rep_org_id	Identificador de la organización
REFERENCE	ref_id	Identificador de la referencia
	descr_txt	Descripción de la referencia
	security_clsfc_code	El valor utilizado es 'NC' (Nato confidential)
	source_txt	Descripción de la fuente
	trans_type_code	El valor utilizado es 'NKN' (Not Known)

**Tabla 9. Tablas y atributos del núcleo común del modelo de datos de SIMACOP**

En la figura 53 se muestra una vista del núcleo común del modelo de datos, tomada directamente de la base de datos del sistema SIMACOP.

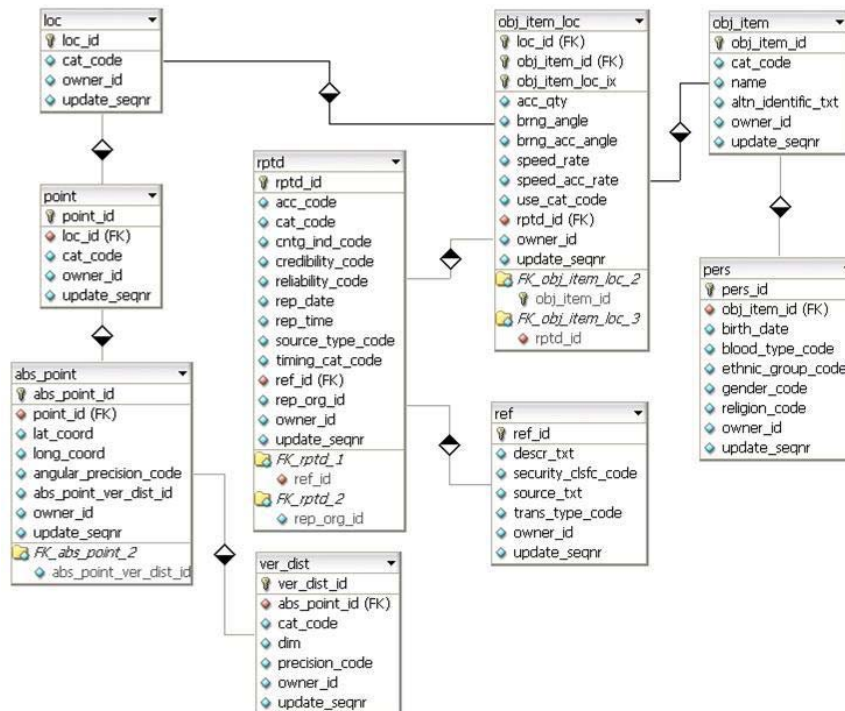


Figura 53

Una descripción del funcionamiento del núcleo común de la base de datos del sistema SIMACOP se puede ver en la figura 54.

En esta figura podemos ver dos procesos distintos, por un lado y marcado con los números en color rojo, podemos ver el proceso de obtención de las posiciones de las unidades desplegadas sobre el terreno.

Se puede ver como estas unidades envían su posición y su identificador al sistema, estas nuevas posiciones se registran en la tabla LOCATION (Ver número 1 rojo en la figura 54).

En cuando estas nuevas posiciones se reciben se la asocia a un identificador de objeto OBJECT-ITEM a través de la tabla OBJECT-ITEM-LOCATION (Ver número 2 rojo en la figura 54), en este caso un identificador de persona, posteriormente se catalogan esas nuevas posiciones con el tipo “punto”, a través de la tabla POINT (Ver número 3 rojo en la figura 54).

Finalmente, una vez catalogadas las posiciones de tipo “punto” con la categoría “punto absoluto”, se almacenan físicamente las coordenadas GPS recibidas en la tabla ABSOLUTE-POINT (Ver número 4 rojo en la figura 54).

Por otro lado, en la figura 54 también se describe una modificación introducida al interfaz de datos de SIMACOP, como fruto de las investigaciones llevadas a cabo en la presente tesis, que permite al sistema SIMACOP la integración de video de alta calidad dentro de su modelo de datos, con esta modificación se puede asociar a determinados reportes de datos su video correspondiente y de esta forma complementar dichos reportes con imágenes.



La descripción del proceso de integración de video en el modelo de datos del sistema SIMACOP queda recogida en color verde en la figura 54.

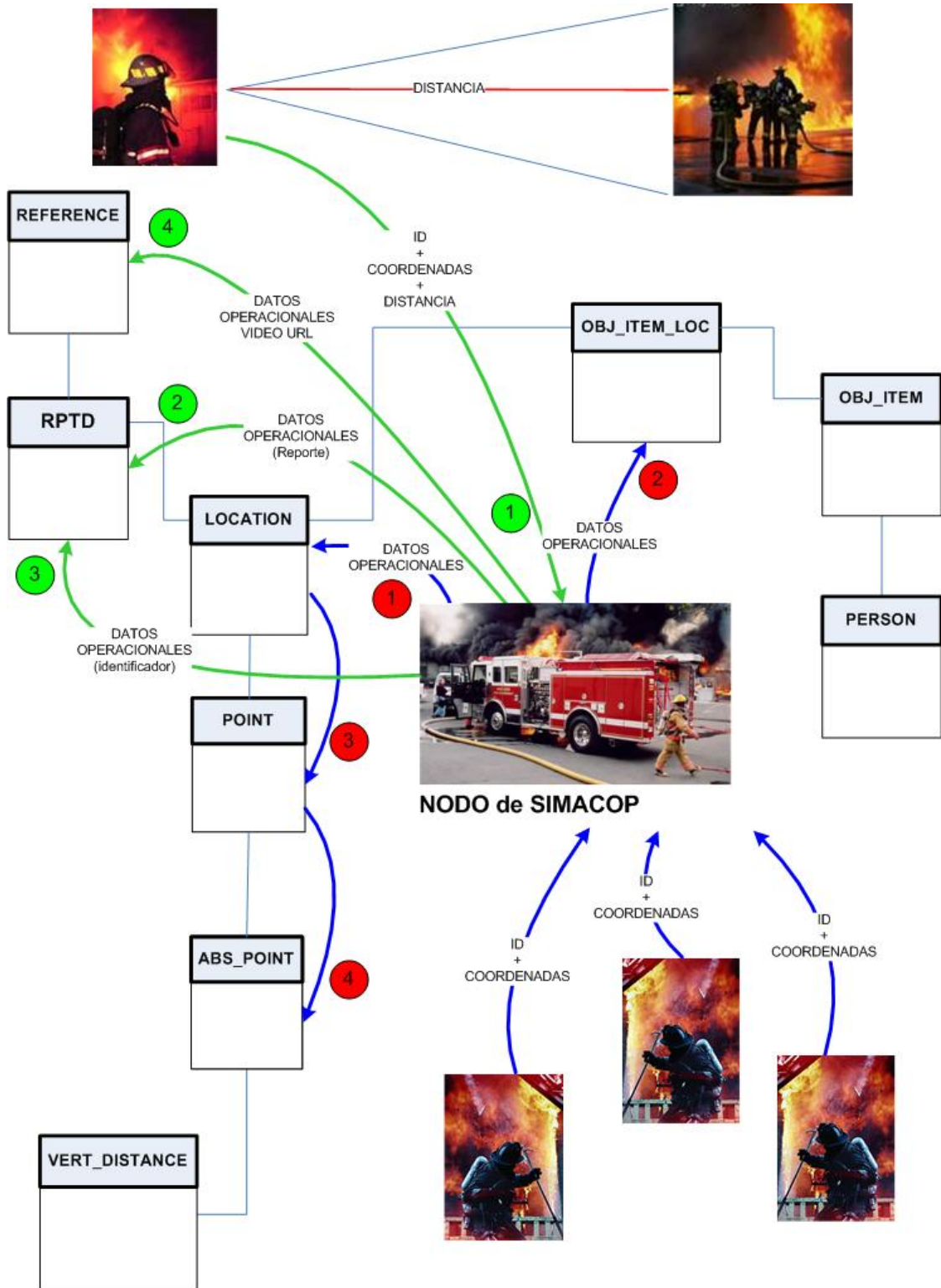


Figura 54

La descripción del proceso de integración de video en el interfaz de datos de SIMACOP sería la siguiente;

Una unidad graba un determinado video en el que se pueden ver unas unidades desconocidas a primera vista. Al sistema se envía la siguiente información:

El identificador de la unidad que ha grabado el video, el video (streaming), que queda almacenado en un servidor de video debidamente etiquetado con su marca de tiempo, la posición de la unidad que ha grabado el video, así como la posición de las unidades grabadas que ha sido calculada con respecto a la de la unidad que ha grabado el video (Ver número 1 verde en la figura 54).

La unidad realiza un reporte de la situación en la que se ha producido la grabación al sistema que queda almacenado en la entidad REPORTING-DATA (Ver número 2 verde en la figura 54).

Posteriormente el sistema almacena el identificador de la unidad que ha grabado el video en el campo “reporting\_organization\_id” de la entidad REPORTING-DATA (Ver número 3 verde en la figura 54).

A su vez sistema almacena automáticamente en el atributo “source\_txt” de la instancia de la entidad REFERENCE asociada a reporte realizado por la unidad que ha grabado el video, una cadena de caracteres de hasta 255 caracteres, que define la URL del video asociado a ese reporte de datos (Ver número 4 verde en la figura 54)

De esta forma queda asociada la instancia del reporte almacenado en la entidad REPORTING-DATA a su video a través del atributo “referente\_id” de la misma instancia.

La modificación realizada al modelo de datos descrita anteriormente, es fruto de las investigaciones llevadas a cabo dentro de la presente tesis doctoral, para permitir la integración de video de alta calidad dentro del modelo de datos del sistema SIMACOP.

El cambio de funcionalidad propuesto no supone una modificación estructural del modelo, es decir, no se han alterado tablas, atributos, ni tipos de atributos para introducir esta nueva funcionalidad.

El cambio consiste en una modificación de tipo funcional del atributo “source\_txt”, ya que solo se cambia la funcionalidad de dicho atributo, que es de tipo cadena de caracteres (string), de la entidad REFERENCE.

Este atributo ya existe en la especificación del modelo de datos y su funcionalidad primigenia es la de describir, de forma textual a través de una cadena de 255 caracteres, la fuente de una determinada referencia.

El cambio de funcionalidad del atributo que se propone en la presente tesis doctoral, consiste en escribir de forma textual, en el atributo “source\_txt”, la URL que apunta al video asociado al reporte de datos asociado a esa referencia, en lugar de la descripción de la fuente de la referencia.

Toda la información recogida en cada nodo del sistema SIMACOP durante las pruebas de campo se replica de forma automática utilizando la aplicación de réplica que implementa el mecanismo DEM que se describió en apartados anteriores de esta tesis.

De esta forma todos los reportes de datos que tengan un video asociado, pueden replicar la URL de ese video a los demás nodos de la red, para que estos videos puedan ser vistos desde dichos nodos.

Los resultados de las pruebas de campo del sistema SIMACOP y su evaluación se verán en los siguientes apartados de la presente tesis.

#### **4.4 Validación del modelo**

En el presente capítulo se mostrarán las descripción de las pruebas de campo realizadas al sistema SIMACOP, así como los resultados obtenidos por SIMACOP y las evaluaciones de los mismos.

Durante las pruebas que se van a describir en este capítulo, se demostrará la viabilidad y buen funcionamiento, de los diseños obtenidos como fruto de la investigación realizada en la presente tesis doctoral y que el sistema SIMACOP lleva incorporados e integrados.

En el presente apartado se van a describir las pruebas de campo y demostradores en los que ha participado el sistema SIMACOP. Las pruebas y demostradores que se van a describir en este apartado son los siguientes:

- Demostración del sistema SIMACOP en el CWID nacional 2006
- Integración de SIMACOP en SIMACET
- Pruebas de interoperabilidad de SIMACOP en el CWID internacional 2007

##### **4.4.1 Demostración del sistema SIMACOP en el CWID nacional 2006**

La demostración de la versión militar del sistema SIMACOP desarrollado por el grupo de investigación de Sistemas de Tiempo Real Distribuidos del Departamento de Comunicaciones de la UPV, se realizó el 3 de mayo de 2006 en la base de la brigada de transmisiones del ejército de tierra en Marines (Valencia).

Como se ha indicado anteriormente, SIMACOP podría dar soporte tanto a acciones militares, como acciones civiles en el ámbito de la gestión de emergencias o en misiones de ayuda humanitaria, por tanto la compatibilidad en acciones conjuntas estaría garantizada, apuntando así directamente a uno de los objetivos nacionales del programa CWID enunciado como *“Ampliación de la funcionalidad de sistemas de mando y control para proporcionar soporte a operaciones que involucren diversas comunidades de interés (COI), militares y civiles, móviles, fija, y remotas, teniendo en cuenta las implicaciones de seguridad multinivel”*.

Tanto en la versión civil del prototipo del sistema SIMACOP, como en la versión militar, solo cambia la presentación y nomenclatura de las unidades en el interfaz de usuario, por tanto el software y el hardware serían idénticos en ambas versiones

En esta demostración se pretende comprobar la viabilidad de un sistema, que ayudará a las personas responsables de una operación (tanto civil como militar), a tener un conocimiento de la situación enriquecido, con información proporcionada por distintos tipos de sensores desplegados sobre el terreno y así poder tomar las decisiones tácticas más adecuadas.

El medio para obtener el adecuado conocimiento de la situación por tanto será:

1) Conocer la situación exacta de las unidades y elementos individuales de cada unidad dentro del espacio de operaciones, mediante la dotación de un receptor GPS en cada elemento individual.

2) Captación de información multimedia, sobre todo vídeo, desde cada elemento individual para “poder ver por sus ojos”. Para ello se requiere dotar a cada elemento individual de una cámara de vídeo o bien de infrarrojos.

3) Adicionalmente, dado el valor de los elementos individuales involucrados, sería muy adecuado poder disponer de información biomédica sobre su estado vital (electrocardiograma y temperatura, al menos). Para ello hace falta dotar a cada elemento individual de los adecuados sensores biométricos.

4) Fusión y transmisión de los datos obtenidos por los distintos sensores al nodo C2 de las unidades por medio de la red de combate. Estos datos serían replicados a los demás nodos de la red táctica de acuerdo a los distintos contratos establecidos a través de la aplicación de réplica basada en el estándar MIP, llevándose a cabo de esta forma una autosincronización de los nodos de la red.

Las características de las operaciones tácticas de pequeñas unidades presentan grandes similitudes con las operaciones de gestión de emergencias civiles, como puede ser por ejemplo, un incendio forestal: se requiere la coordinación de pequeñas unidades, siendo a menudo muy útil la capacidad de autosincronización en tiempo real de estas unidades.

Evidentemente, la naturaleza del enemigo varía (de los miembros de una unidad terrorista o de guerrilla urbana a los frentes de un incendio...) y la forma de ubicar su posición y responder a su línea de acción también es distinta. Sin embargo, parece adecuado pensar, con pequeñas variaciones, en la dualidad del sistema propuesto en los ámbitos de uso militar y de gestión de emergencias civiles.

#### **4.4.1.1 Descripción funcional de la demostración**

SIMACOP es un sistema de seguimiento de fuerzas amigas basado en tecnologías COTS, con capacidad de transmisión, réplica y fusión de flujos de datos multimedia, incluido streaming de vídeo.

El sistema que se va a desplegar en la demostración consiste en varios nodos C2, conectados entre sí y con los elementos individuales con funcionalidad de sensores/actuadores, mediante una red de datos inalámbrica de elevada capacidad (decenas de Mbps), basada en el estándar IEEE 802.11 WIFI en el prototipo funcional actual con previsión de migración a IEEE 802.16 WiMax [79].

El planteamiento funcional del sistema que se va a demostrar se resume en los siguientes puntos:

- Cada miembro individual (jefe de pelotón y unidades de tropa) está dotado de un SBC (Single Board Computer), que fusiona las informaciones de distintos sensores (cámara de vídeo o de IR, GPS, biosensores, designadores de posición de las unidades enemigas y neutrales) y genera un solo flujo de información por cada elemento individual.
- Los SBC de cada unidad individual están conectados entre sí mediante una red inalámbrica “ad hoc” de tal forma que el jefe de pelotón recibe, fusiona y retransmite los flujos de cada unidad de tropa (y el suyo propio) al nodo SIMACOP de C2 de primer nivel. En caso de caída o fallo del jefe de pelotón la red se autoconfigura y se elige otro punto de enlace con el nodo C2 de nivel superior.

- La aplicación del nodo de primer nivel de C2 produce la COP a nivel de sección ya que recibe los flujos de datos de los pelotones que conforman la sección. La conexión de este puesto de mando de sección con los distintos pelotones también se consigue a través de una red de datos inalámbrica. La aplicación C2 se ejecutaría sobre un PC portátil militarizado con conexión inalámbrica.

Un nodo C2 de primer nivel (sección/pelotones) puede operar de tres modos:

- De forma aislada cuando por la dimensión de la operación, no se requieren más niveles de C2. Se genera una única COP a nivel de sección/pelotones.
- De forma autosincronizada con otros nodos C2 involucrados en la operación. Para ello se requiere una aplicación de réplica de la información de los distintos nodos que forman la red. Se necesitará por tanto conectividad total de red inalámbrica entre los nodos C2 de nivel de sección involucrados. Se genera de esta forma una COP entre los distintos nodos C2
- Bajo la jerarquía de un puesto C2 de nivel superior que coordina a varios nodos C2 de nivel de sección/pelotones. Se requiere una aplicación de réplica de la información de los distintos nodos que forman la red. Para ello es necesaria la conectividad total de red inalámbrica entre los nodos C2 de nivel de sección/pelotones involucrados y el puesto de mando de nivel superior, que denominaremos “nivel de secciones”. Se genera un COP entre los distintos nodos C2 de nivel de sección y el de nivel superior.

En el despliegue realizado para la prueba se ha optado por el tercer modo de operación del nodo de C2 de primer nivel.

Para una mayor ilustración funcional de la demostración, a continuación se incluyen las cuatro pantallas de la aplicación de los nodos C2.

Estas pantallas están capturadas del prototipo en su estado actual e incluyen: cartografía vectorizada, botones de acceso al nivel inferior y superior, imagen de vídeo procedente de la cámara de un elemento individual seleccionado así como las constantes vitales de dicho elemento.

A los elementos/niveles de sección, pelotón y unidad de tropa (JP por jefe de pelotón, y UT por unidad de tropa) se puede acceder pulsando el correspondiente botón o pulsando sobre el icono superpuesto a la cartografía del teatro de operaciones.

Hay que notar, que cuando se realizó esta demostración, la aplicación de replica basada en el estándar NFFI no había sido implementada todavía, por lo tanto todas las réplicas de información que se realizaron durante la demostración fueron mediante la aplicación de réplica que implementa el estándar MIP. La aplicación de réplica de datos MIP permite la autosincronización de los nodos C2 de sección, la persona al mando de una sección “ve” a su propia sección y “ve” también al resto de secciones, porque comparten la misma información almacenada en su interfaz común de datos.

Las pantallas de los distintos niveles jerárquicos del sistema SIMACOP desplegado en la demostración se pueden ver en las siguientes figuras.

En la figura 55 se puede ver la pantalla del nodo SIMACOP de C2 a nivel de secciones.

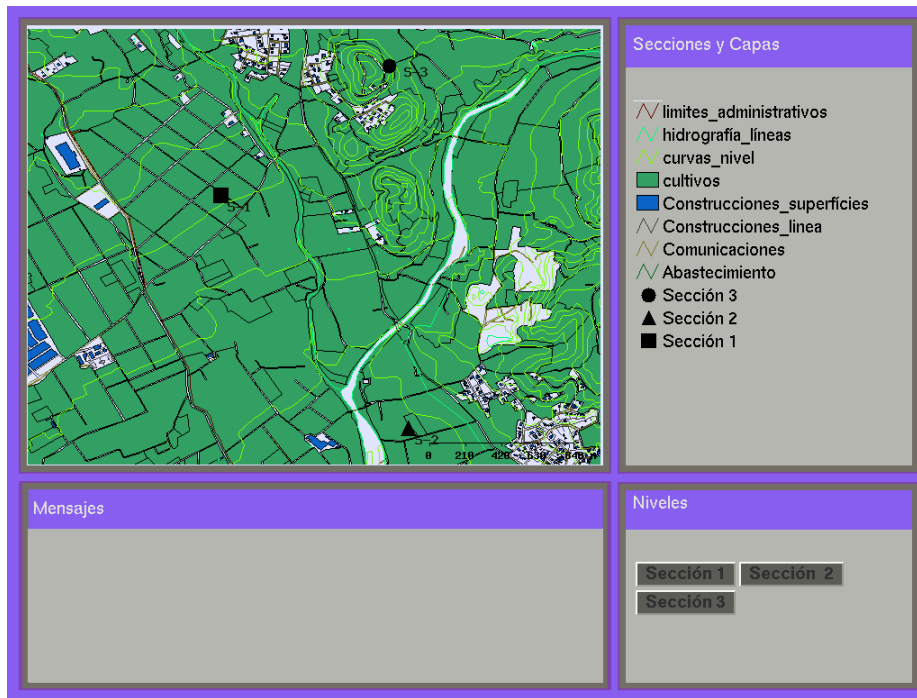


Figura 55

En la figura 56 se puede ver la pantalla del nodo SIMACOP de C2 a nivel de sección/pelotones

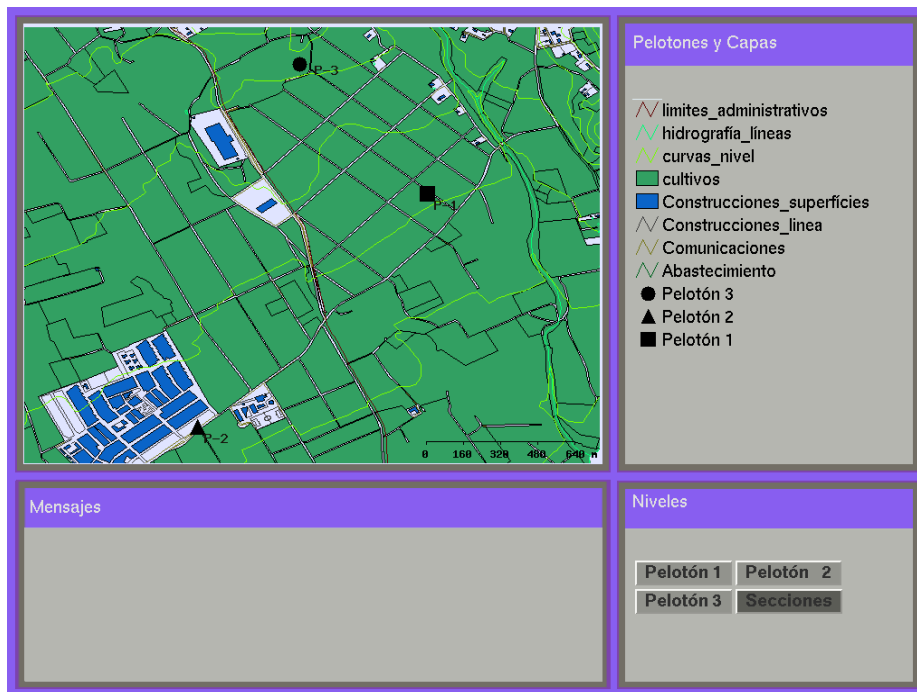


Figura 56

En la figura 57 se puede ver la pantalla del nodo SIMACOP de C2 a nivel de pelotón/unidades de tropa.

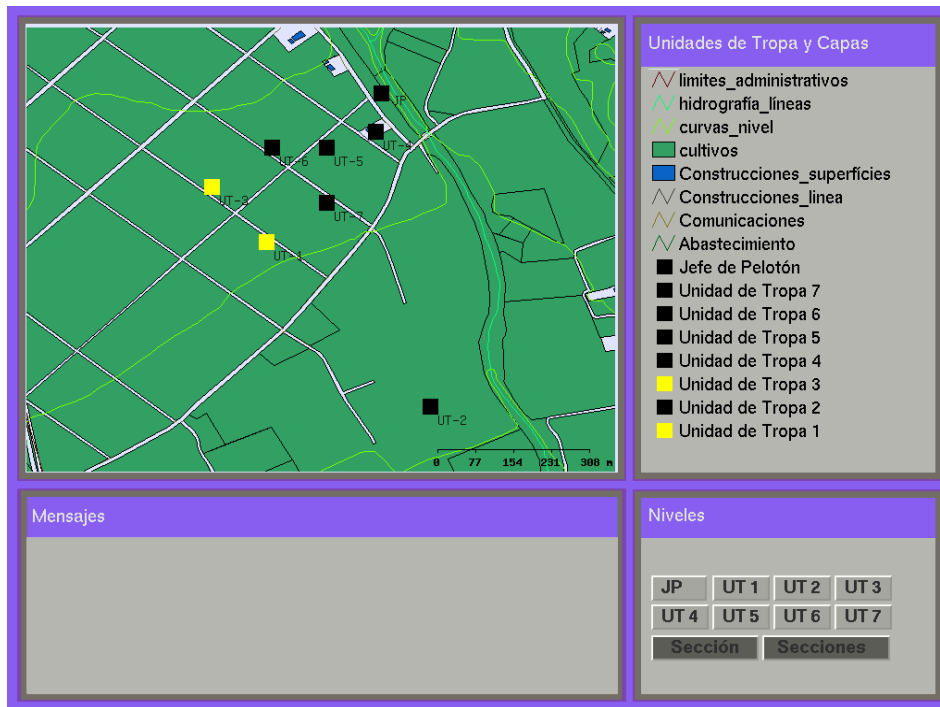


Figura 57

En la figura 58 se puede ver la pantalla del nodo SIMACOP de C2 a nivel de unidad de tropa

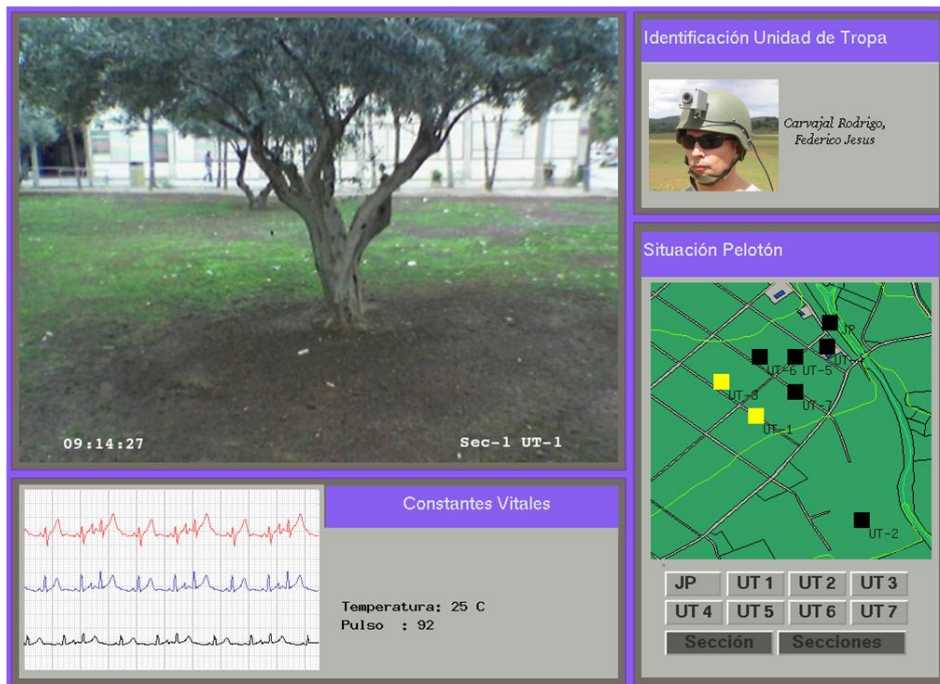


Figura 58



El prototipo del sistema SIMACOP que se desplegó en la demostración incluye la funcionalidad de monitorización del estado vital de cada unidad de tropa. Si las constantes vitales de una unidad, captadas por los biosensores se deterioran, el icono de la unidad de tropa pasa de color negro (estado operativo) a amarillo (alarma) y de ahí a rojo (unidad no operativa), según el grado de deterioro de las constantes, esta funcionalidad se puede ver en la parte inferior derecha de la figura 58.

#### 4.4.1.2 Descripción técnica de la demostración

En este apartado se van a describir con detalle algunas de las tecnologías utilizadas en la demostración del sistema SIMACOP.

Se ha desarrollado un prototipo de nodo C2 y de equipamiento individual de cada unidad de tropa, que incluye las siguientes tecnologías, todas ellas COTS:

- Cámaras de vídeo y tarjetas digitalizadoras/capturadoras
- Biosensores: electrocardiográfico, pulso y temperatura.
- GPS
- SBC con sistema operativo Linux (distribución con componentes mínimos)
- Módulo SW de codificación MPEG-4 y streaming de vídeo
- Módulo SW de réplica de datos
- Conectividad Bluetooth y coaxial
- Computador personal (nodo C2) con sistema operativo Linux
- Servidor web Apache
- GIS Mapserver
- Conectividad IEEE 802.11 WiFi.

El esquema de nodo C2 descrito anteriormente se puede ver en la figura 59.

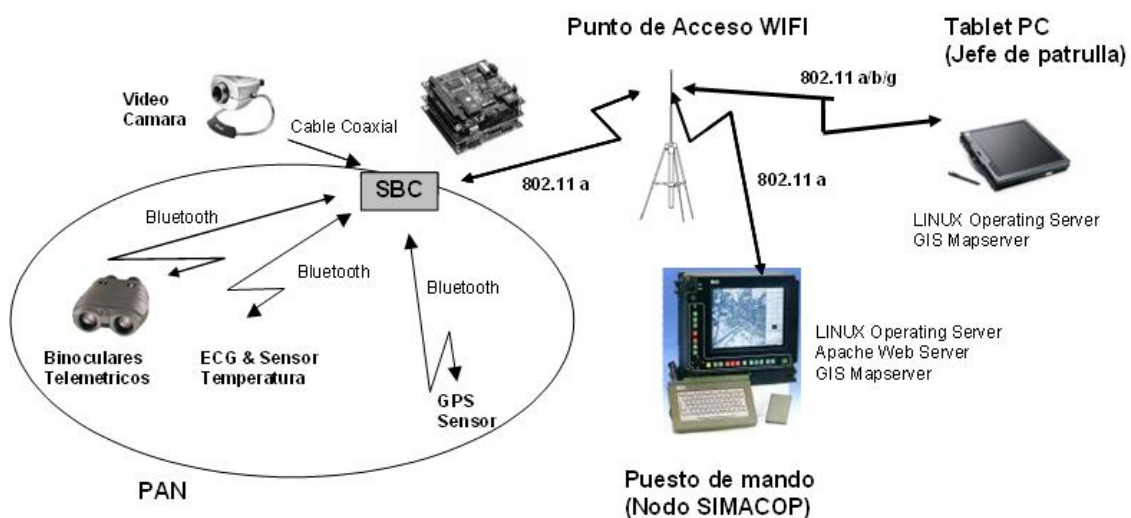


Figura 59

A continuación pasaremos a describir la arquitectura del sistema desplegado en la demostración CWID 2006 y posteriormente identificaremos todos los elementos de la figura con fotografías reales de la demostración, que fue llevada a cabo con éxito.

Los componentes de la arquitectura desplegada son los siguientes:

- Un nodo de segundo nivel (Secciones) con un puente WIFI para conectar con los dos nodos de primer nivel con el objeto de replicar los datos actualizados en el interfaz común de datos y tener una COP más amplia.
- Dos nodos de primer nivel (Sección/Pelotones), con sus propios puntos de acceso WIFI conectados con sus patrullas y un puente WIFI para conectar los dos nodos con el objeto de replicar los datos actualizados en el interfaz común de datos.
- Una patrulla real compuesta por dos soldados con su completo equipamiento (SBC con enlace WIFI, GPS, video cámara en el casco, sensores biométricos y un tablet PC para el jefe de la patrulla).
- El resto de los elementos de la demostración son simulados.

Todos los elementos mencionados se pueden ver en el esquema del despliegue realizado de la figura 60.

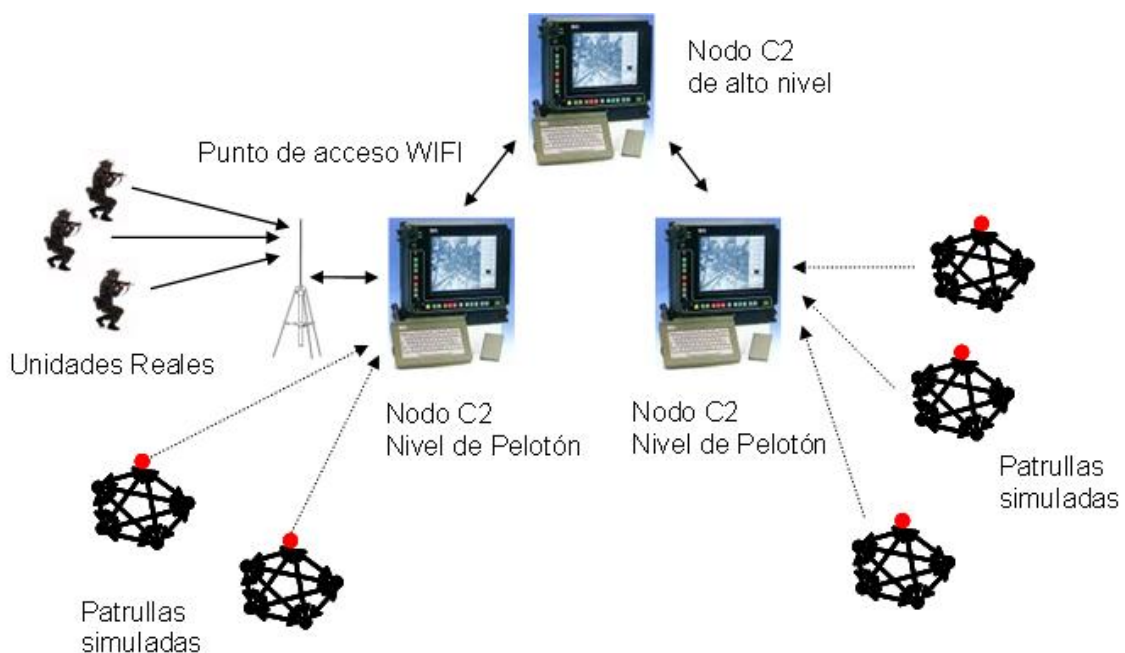


Figura 60

En las siguientes figuras, se pueden ver los distintos elementos descritos anteriormente en fotografías reales tomadas durante el desarrollo de la demostración del prototipo, la cual como se ha dicho anteriormente y como se verá en su evaluación fue llevada a cabo por el con éxito por el grupo de investigación de Sistemas de Tiempo Real Distribuidos del Departamento de Comunicaciones de la UPV.

En la figura 61 podemos ver la patrulla compuesta por las dos unidades de tropa del regimiento de transmisiones 21, con todo el equipamiento descrito anteriormente.



**Figura 61**

Detalles del tablet PC y de los sensores biométricos se pueden ver en las figuras 62 y 63.



**Figura 62**



**Figura 63**

En la figura 64 podemos ver un vehículo del tipo, Rioja especialmente dedicado a las comunicaciones. En este vehículo se han instalado las antenas sectoriales (Ver número 1 en la figura 64), que cubrirán el enlace WIFI entre las unidades de tropa y el nodo C2 de SIMACOP de nivel de Sección/Pelotones (Ver número 3 en la figura 64), que las monitoriza y que replica la información que recibe de ellas a los demás nodos de la red.

Esta réplica de información hacia los demás nodos de la red se realiza a través de la antena parabólica (Ver número 2 en la figura 64) también instalada en el vehículo y que cubre el enlace WIFI entre el nodo C2 de nivel de Sección/Pelotones y el nodo C2 de nivel de secciones.



**Figura 64**

En la figura 65 podemos ver el nodo de nivel de Secciones (Ordenador de la izquierda) y el segundo nodo de nivel de Sección/Pelotones (Ordenador de la derecha), que se encuentra dentro del cuartel de la brigada de transmisiones, ya que la información que este segundo nodo de nivel de Sección/Pelotones aporta a la demostración es simulada. El nodo de nivel de secciones hace las veces de puesto de mando retrasado donde se tomarían las decisiones para dirigir la operación.

Como puede verse en la figura, ambos ordenadores tienen en sus interfaces la misma información replicada desde el nodo de nivel de Sección/Pelotones avanzado y que les indica tanto la posición y estado de las unidades de tropa, como el video tomado por estas unidades.



**Figura 65**

Como ya se ha mencionado anteriormente en este apartado, en la fecha en la que se realizó esta demostración del sistema SIMACOP, la aplicación de réplica basada en el estándar NFFI y que permite la réplica de la información de posicionamiento entre distintos sistemas de FFTS, no estaba operativa y todas las réplicas de datos realizadas por el sistema SIMACOP, en la demostración nacional CWID 2006 se realizaron a través de la aplicación de réplica que implementa el estándar MIP de interoperabilidad entre sistemas C2IS. Aplicación que se desarrolló como parte de las investigaciones realizadas durante la presente tesis doctoral.

Un detalle de la transmisión de video en directo desde el nodo C2 avanzado lo podemos ver en la figura 66, donde podemos ver que mientras en el nodo de nivel superior (Ordenador de la izquierda), se siguen viendo las posiciones de las unidades de tropa, en el segundo nodo de nivel Sección/Pelotones (Ordenador de la derecha) se puede ver el video y las posiciones de las unidades de tropa (esquina inferior derecha del PC de la derecha) replicadas desde el nodo de nivel de Sección/Pelotones avanzado.

Cabe destacar, como puede verse en la figura 66, la alta calidad de la imagen del video que proporciona el sistema SIMACOP pese al poco ancho de banda que consume su streaming de video, esto se debe a su óptimo algoritmo de compresión.



**Figura 66**

Como puede verse por las imágenes tomadas durante el transcurso de la demostración y por la evaluación a la que se sometió al sistema al terminar la prueba, la cual se mostrará en los apartados siguientes de la presente tesis doctoral, la demostración fue un éxito, funcionando perfectamente todo el sistema.

La evaluación del sistema se realizó mediante un cuestionario, que fue rellenado por observadores militares pertenecientes a distintas armas del ejército de tierra, que asistieron al desarrollo de la demostración.

Como partes esenciales del sistema que se desplegó, podemos mencionar el correcto funcionamiento de la aplicación de réplica de datos y del interfaz de datos común, que fueron desarrollados como parte de las investigaciones llevadas a cabo dentro de la presente tesis doctoral.

#### **4.4.2 Evaluación de SIMACOP en su demostración en el CWID nacional 2006 (EP-31 CWID06)**

De las quince preguntas efectuadas a los observadores de la prueba del sistema SIMACOP y calificadas de 1 a 5, de peor a mejor, se exponen los resultados de la evaluación:

- Calidad percibida del vídeo en el puesto de mando 4.5
- Calidad en la distinción de obstáculos y características del terreno 4.6
- Nivel de confianza del posicionamiento de los efectivos 4
- Valoración de la percepción de la situación desde el PC. 4
- Valoración de la COP para la toma de decisiones 4.1
- Valoración como ayuda a la toma de decisiones 4.5
- Facilidad de utilización de la aplicación. 4.5
- Valoración de la utilidad del tablet PC al Jefe de Pon. 4.2
- Valoración de la información del estado vital de los efectivos 3.3
- Valoración de la ergonomía para el soldado 3.3
- Operatividad del sistema para el Jefe de Pon. 4
- Operatividad del sistema para el PC. 4.3
- Valoración del funcionamiento de forma aislada. 4.1
- Valoración del funcionamiento autosincronizado. 4.4
- Valoración del funcionamiento jerárquico. 4.4

#### **Como puntos fuertes a destacar:**

- La apreciación global de este sistema es muy buena y se ve que tiene un campo interesante a seguir desarrollando en el seguimiento y ayuda al Jefe de Pelotón y Jefe de Sección para dirigir sus efectivos.
- Destaca el GIS y la representación gráfica de obstáculos, edificios y la situación de los efectivos. Pues se abre un gran campo para la ayuda a la toma de decisiones a bajo nivel del Jefe de Sección y Pelotón para avanzar, defender y sobre todo saber si sus efectivos están vivos y dónde.
- Es sencillo de manejar con un interfaz muy intuitivo. Siendo destacable que emplee linux como sistema operativo, pues es de libre difusión con lo que los costos de adquisición son menores y es un sistema operativo potente y fiable con una gran cantidad de librerías en el mercado a libre disposición.



- Es muy interesante la capacidad de captar vídeo, pues facilita la comprensión en el PC. de lo que está sucediendo dónde está el soldado, observatorio o vehículo de exploración. Sobre todo de cara a la inteligencia militar y la 2ª sección que puede valorar mejor la situación en la faceta del enemigo.

#### **Como puntos débiles:**

- El soporte de comunicaciones no es el adecuado, la prueba se hizo con un enlace de Wifi, dando limitaciones en alcance y coberturas. Sería recomendable tomar dos opciones:
- Para mantener la capacidad de captar vídeo habría que probar con la versión de Wimax que está a punto de salir al mercado, tal como apunta la Universidad Politécnica de Valencia.
- Con objeto de mejorar los alcances se debería pasar la información de posición, vital, la de designación de enemigo, etc. toda menos el vídeo, que requiere un ancho de banda mayor que los datos simples, por vía radio VHF.

#### **OBJETIVOS Y MEJORAS**

Este sistema se estima que es de aplicación en el ámbito militar y muy recomendable en misiones y en ejercicios.

#### **Como objetivos a alcanzar se proponen:**

- Interoperabilidad con SIMACET.
- Fusión de flujos de datos de sensores no humanos (UAV, de helicópteros, de vehículos de exploración, de infrarrojos, sísmicos y de puestos de radar rasura de las Unidades de Infantería.
- Representación de la posición de Unidades enemigas en la COP. La captación de la posición de estas y su identificación para evitar duplicidades en el sistema.
- Utilizar como soporte de datos alternativo la radio en VHF.
- Probar Wimax en su versión IEEE 802.16e.

#### **Como mejoras del sistema se proponen:**

- Probar la tecnología bluetooth (manos libres) en el equipo del soldado y eliminar los cableados.
- Probar sistema de baterías recargables de larga duración y poco peso que aumenten la autonomía de los equipos.
- Probar un sistema de recarga por placas solares portátiles.
- Mejorar la representación de la COP, con la posibilidad de insertar nuevos símbolos.

- Interesa saber cuándo se capta la señal de vídeo de un soldado conocer el campo de visión de abarcar y la orientación, que sería recomendable se pudiese ver reflejada en la COP.
- Mejorar la interfaz de la información vital del soldado mostrando mediante unos colores su estado de salud y la acción a tomar. Ejemplo malherido pero puede aguantar en amarillo, o muy grave necesita evacuación urgente en rojo, fallecido en negro y en buen estado de salud en verde.
- Posibilidad de enviar órdenes tipo misión a cada uno de forma que no sea necesaria la reunión del personal para explicar la orden pero si se entienda en el gráfico del jefe de pelotón y puedan actuar coordinadamente.

### CONCLUSIONES

- Se recomienda este sistema para empleo en el Ejército de Tierra, pero para llegar a ser un prototipo operativo debería haber salvado el problema de la cobertura y movilidad de las estaciones base (Puestos de Mando de Pelotón). Actualmente se considera demasiado crítico el enlace de wifi como para considerar seriamente su empleo tal como se ha hecho la demostración.
- Puede ser aplicado a todo tipo de Unidades que dispongan de personal que deseen tener bajo control. Estas podrían ser Infantería de Marina, Unidades de emergencias (bomberos, puestos de control de carreteras, observatorios de Infoca.)
- Es una idea muy buena y necesita ser desarrollada más en profundidad pues llena una laguna de información muy importante que es el control a bajo nivel. Hasta ahora tenemos en desarrollo el programa Lince para el control de vehículos acorazados / mecanizados pero poder tener un sistema ligero, sencillo y robusto que ofrezca estas posibilidades nos brinda la posibilidad de tener un conocimiento más exacto de la situación a bajo y no “estar ciego” en el PC.
- Debemos seguir con atención los avances de SIMACOP en cuanto gane cobertura y flexibilidad en las comunicaciones pues es un elemento único dentro del actual marco de herramientas para ayuda al mando y control de las Pequeñas Unidades.

Durante la demostración nacional CWID 2007, cuya evaluación oficial se muestra en este apartado, el sistema SIMACOP utilizó el modelo de datos propuesto en la presente tesis doctoral, como núcleo de su base de datos.

El resultado exitoso la prueba, así como la buena valoración del sistema por parte de los evaluadores militares presentes en la demostración, valida el modelo de datos utilizado en un entorno multinacional.

La validación del modelo de datos se fundamenta en las siguientes afirmaciones:

- El hecho que el modelo de datos de SIMACOP esté basado en el estándar MIP le permitió una correcta réplica de datos que contribuyó de forma decisiva al éxito de la prueba.

- La réplica de los datos del puesto avanzado al puesto retrasado funcionó correctamente actualizándose las posiciones de las fuerzas amigas sobre el terreno en tiempo pseudo real
- Las posiciones de las fuerzas amigas recibidas desde las unidades de tropa fueron almacenadas correctamente en la base de datos y pudieron visualizarse correctamente en la pantalla de SIMACOP.

#### **4.4.3 Integración de SIMACOP con SIMACET**

Tras las pruebas del sistema SIMACOP en la demostración nacional CWID 2006, se mantuvieron diversas reuniones con los mandos militares vinculados con el programa CWID y con las personas de contacto de la empresa ISDEFE [80] asignadas también a dicho programa.

Como resultado de dichas reuniones se elaboró un calendario de trabajo con el objetivo de integrar el sistema SIMACOP, como sistema de seguimiento de fuerzas amigas (FFTS), en el sistema de mando y control del ejército de tierra SIMACET.

Para llevar a cabo dicho objetivo se utilizaron parte de los desarrollos implementados durante la presente tesis doctoral.

Durante los contactos posteriores mantenidos entre mandos militares del ejército de tierra y los profesores responsables del grupo de investigación de Sistemas y Aplicaciones de Tiempo Real Distribuido de la Universidad Politécnica de Valencia (UPV), se determinó que el esquema de funcionamiento de ambos sistemas (SIMACOP/SIMACET), una vez se hubiera llevado a cabo su integración, sería el descrito en el esquema que se muestra en la figura 67.

En primer lugar SIMACOP recibiría las posiciones de las fuerzas amigas desde los distintos sistemas de seguimiento de fuerzas amigas (FFTS) de otros países utilizando su aplicación de réplica basada en el estándar NFFI.

Estos datos de posicionamiento se almacenarían en la base de datos NFFI de SIMACOP para ser mapeados posteriormente en el interfaz de datos compatible MIP de SIMACOP.

A su vez el sistema SIMACOP recibe los datos de posicionamiento de sus fuerzas propias, los cuales se almacenan directamente dentro del interfaz de datos de SIMACOP y posteriormente son mapeados por la aplicación de réplica dentro de la base de datos NFFI para ser replicados automáticamente a los sistemas FFTS de los países que participen en la operación.

Desde el interfaz de datos de SIMACOP se mapearán todos los datos de posicionamiento, (los recibidos desde otros sistemas FFTS a través de mensajes NFFI, así como los de las fuerzas propias), al modelo de datos (MDC2ET versión 1.7) del sistema de mando y control del ejército de tierra SIMACET.

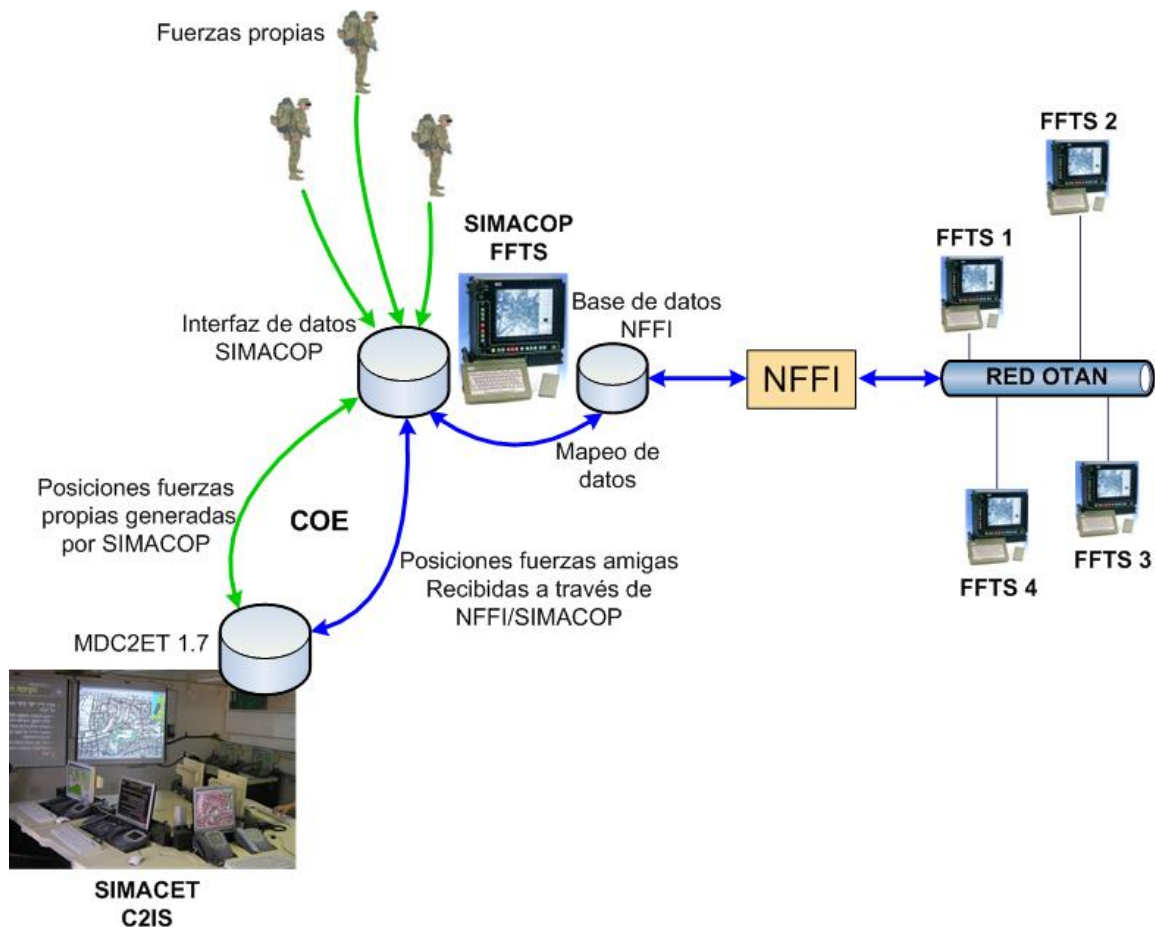
Este modelo de datos es el fruto del siguiente proceso:

Sobre la base del modelo LC2IEDM 2.0 de MIP se añaden y modifican elementos para obtener el MDC2ET 1.7. En la documentación internacional adjunta proporcionada por el ejército de tierra se detalla la explicación de los diferentes elementos del modelo internacional MIP, que se mantienen en el nacional.

En la documentación nacional adjunta proporcionada por el ejército de tierra se detallan solamente las modificaciones que se realizan en el LC2IEDM 2.0 de MIP para obtener el MDC2ET 1.7.

En el modelo erwin facilitado por el ejército de tierra, se pueden observar resaltadas en color en rojo las extensiones añadidas al modelo de datos LC2IEDM 2.0 para obtener el MDC2ET 1.7. Las entidades que tienen alguna modificación están renombradas con el prefijo SMC.

Como también se puede observar en el esquema que se muestra en la figura 67, para llevar a cabo la interconexión entre el interfaz de datos de SIMACOP y el modelo de datos MDC2ET 1.7 de SIMACET se utilizará la herramienta Common Operating Environment (COE) [81] [82].



**Figura 67**

Para aclarar un poco más algunos conceptos se va a describir en este apartado, que es y cómo se utiliza en la integración entre SIMACOP y SIMACET, la infraestructura de información de defensa en un entorno común de operativo o Defense Information Infrastructure (DII) Common Operating Environment (COE).

El DII COE es la herramienta de interconexión del sistema de mando y control del ejército de tierra SIMACET, fue desarrollado a finales de 1993 para eliminar la duplicación de desarrollos en áreas como el mapeo de datos, la gestión del seguimiento de fuerzas y los interfaces de comunicación [83], así como para eliminar incompatibilidades de diseño entre los sistemas del departamento de defensa (DoD) de los Estados Unidos.

Conceptualmente hablando COE es diseñado para reducir el coste de programación y los riesgos de la reutilización soluciones software probadas así como facilitar el hecho de poder compartir funcionalidades comunes entre sistemas ya existentes y los nuevos diseños de sistemas, en lugar de desarrollar los sistemas desde el principio como se venía haciendo hasta entonces.

El objetivo final de COE es aumentar las capacidades de los sistemas en términos de interoperabilidad, reusabilidad, portabilidad y capacidad operacional, reduciendo a su vez el tiempo de desarrollo, la obsolescencia técnica, los requerimientos de formación para el personal encargado del manejo de los sistemas y el coste total del ciclo de vida de los nuevos sistemas desarrollados.

DII COE reutiliza probados componentes software de programas y servicios existentes para facilitar funciones comunes de mando, control, comunicaciones, computación e inteligencia o Command, Control, Communication, Computer and Intelligence (C4I) a los nuevos diseños.

COE quiere enfatizar la reutilización del software y los datos así como la interoperabilidad para los mismos, pero además el concepto de diseño de COE abarca las siguientes características:

- Una arquitectura de sistemas interoperables (plug and play).
- Interfaces comunes persona/máquina.
- Componentes software y datos reutilizables.
- Estrictos requerimientos de seguridad.

Por todo lo dicho anteriormente, podemos decir que el objetivo principal del estándar COE es establecer funciones comunes de los sistemas que puedan ser extraídas e implementadas como un conjunto de bloques compatibles de bajo nivel para poder ser usados de una forma sencilla por los diseñadores e integradores de sistemas.

La interoperabilidad entre sistemas, que es el caso que nos ocupa en este apartado, puede verse significativamente mejorada por el hecho de que un software común pueda ser usado por varios sistemas para implementar funciones comunes. Con el uso de COE los calendarios de desarrollo pueden ser acelerados y se pueden conseguir sustanciales ahorros en costes de desarrollo.

La taxonomía de COE define dos niveles de componentes software reutilizables;

- Servicios de infraestructura, que incluyen el núcleo (Kernel) de servicios DII COE.
- Sistemas operativos basados en la filosofía commercial-off-the-shelf (COTS).

La infraestructura de servicios se encarga de las funciones que hacen posible el movimiento de los datos a través de la red e incluye servicios de computación distribuida y servicios Web. El núcleo facilita servicios de bajo nivel incluyendo un entorno visual de gestión, herramientas de gestión y un sistema básico de administración de la seguridad.

Para finalizar este apartado donde se expone la descripción entre los sistemas SIMACOP y SIMACET, hemos de decir que no se describe con detalle en la presente tesis doctoral, el modelo MDC2ET 1.7, ni se muestra las estructuras de datos del modelo LC2IEDM 2.0, que han sido modificadas para su adaptación como modelo de datos del sistema SIMACET, por ser considerado información clasificada

Para llevar a cabo las pruebas necesarias de integración de los dos sistemas en los laboratorios de la UPV, el ejército de tierra facilitó dos ordenadores portátiles con el programa SIMACET instalado, así como el modelo de datos MDC2ET 1.7 y documentación complementaria.

Los resultados de la integración de los dos sistemas se probaron en experimentos de laboratorio con un éxito total a la hora de interoperar ambos sistemas.

#### **4.4.4 Pruebas de interoperabilidad NFFI del sistema SIMACOP en la demostración internacional CWID 2007**

En este apartado se va a describir el plan de actividades que se han realizado durante el ejercicio NATO BFSA-III (NBFSA-III), dentro de la demostración del programa Coalition Warrior interoperability Demonstration (CWID) 2007 realizada en Jørstadmoen (Noruega). Este plan de actividades ha sido desarrollado por la NATO Consultation, Command and Control Agency (NC3A) y ha sido usado como Trial Definition and Plan (TDP), durante el ejercicio NBFSA-III.

Desde el punto de vista de la NC3A esta demostración forma parte del proyecto “Friendly Force Tracking Experimentation” llevado a cabo dentro del 2007 Experimentation Programme of Work (EPOW) por el Allied Command Transformation (ACT). Este proyecto es la continuación del trabajo realizado por la NC3A durante 2005 y 2006 [84], bajo EPOW en apoyo del Friendly Force Information (FFI) Working Group (FFIWG), dirigido por la división de ACT Joint Experimentation, Exercises and Assessment (JEEA).

El principal objetivo del proyecto es conducir los experimentos sobre interoperabilidad NFFI entre sistemas de seguimiento de fuerzas amigas (FTS) de las naciones participantes, las naciones con representación gubernamental y/o industrial en la demostración son las siguientes: Francia, Italia, Alemania, España, Noruega y Rumania.

##### **4.4.4.1 Descripción los objetivos e hitos de la demostración internacional CWID 2007**

En concreto, el principal objetivo de la demostración NBFSA-III es probar y demostrar los siguientes conceptos:

- La interoperabilidad NFFI entre los sistemas FTS de las naciones participantes y la próxima difusión de los datos en tiempo real en un plazo corto/medio de tiempo.
- El acceso a los datos obtenidos por estos sistemas FTS por parte de otros sistemas de mando, control e información (C2IS) de la OTAN.

Para conseguir el objetivo principal del ejercicio se deben de cumplir los siguientes objetivos operacionales durante la demostración:

- Revisar y consolidar la actual especificación del estándar NFFI v1.3, en particular se revisarán con interés los siguientes aspectos del estándar:
  - El formato de intercambio de los datos
  - Los perfiles del servicio de interoperabilidad o Service Interoperability Profiles (SIP): IP1 e IP2.
- Identificar las necesidades y definir una mejora y extensión de las especificaciones NFFI en función de las lecciones aprendidas desde el CWID 2006 y otros experimentos relacionados.
- Probar, validar, revisar y consolidar, durante las pruebas de la demostración, las nuevas especificaciones realizadas estándar NFFI.



- Ampliar la coordinación y el consenso sobre el uso de NFFI, extendiendo la participación de las naciones en las demostraciones NBFSA.

El campo de acción de la demostración de interoperabilidad CWID 07 es principalmente técnico e incluye los siguientes hitos:

- La definición del interfaz NFFI para ser usado en el intercambio y compartición de datos de los seguimientos de las fuerzas amigas, entre los sistemas FTS de los países participantes en la demostración y de la OTAN.
- La validación, a través de la experimentación en laboratorio, del estado compartido situación de las fuerzas terrestres que se consigue a través e los intercambios de mensajes NFFI entre los sistemas FTS.
- La evaluación de la viabilidad técnica, las limitaciones y el diseño del interfaz NFFI cuando se utilice en los sistemas FTS ya existentes.

Para llevar a cabo todos los objetivos e hitos descritos anteriormente se llevarán a cabo durante la demostración CWID 07 diversos ejercicios o pruebas de interoperabilidad entre los sistemas FTS reales que participan en la demostración.

Los ejercicios de interoperabilidad en los que participe el sistema SIMACOP, se describirán con detalle durante el presente apartado y los resultados y la evaluación de los mismos se expondrán en los siguientes apartados de la presente tesis doctoral.

#### **4.4.4.2 Requerimientos necesarios para la demostración CWID 2007**

La principal guía de requerimientos para la demostración CWID 2007 son las recomendaciones para la experimentación recogidas en el informe CWID-06 NBSA Experimentation Report [84].

En este apartado vamos a resumir los principales requerimientos que tienen que observar los sistemas FTS presentes, para participar en las pruebas de la demostración CWID 2007:

1. Extensión de los perfiles del servicio de interoperabilidad o Service Interoperability Profiles (SIP), dando un paso de esta forma hacia la implementación de una arquitectura orientada a servicios. En la actual especificación NFFI los únicos SIPs definidos son el IP1 y el IP2, que son perfiles TCP/IP y UPD relativamente simples para intercambiar los datos NFFI. La implementación de estos SIP's es simple y eficiente, pero también tienen una funcionalidad muy limitada. Otro SIP llamado IP3, basado en la tecnología de interfaz de servicios web, fue definido y parcialmente probado durante la demostración CWID 2006 [85].

El IP3 incluye el requerimiento de pedir datos o “pulling”, principalmente por parte de los sistemas clientes, que necesitan actualizar la representación de la situación del espacio de operaciones a intervalos fijos de tiempo. La extensión de este SIP con funcionalidades adicionales permitiría la definición e implementación de un interfaz común orientado a servicio para los sistemas FTS utilizados por las distintas naciones de la OTAN.

La simplicidad y la flexibilidad son características indispensables en la especificación y la implementación del interfaz.

Para continuar el buen camino marcado por las demostraciones CWID 05 y CWID 06 el coste de la implementación de la especificación NFFI ha de mantenerse lo más bajo posible, esto se puede conseguir siguiendo una implementación y un diseño simples que permitan múltiples opciones y una aproximación incremental de la implementación.

2. Soluciones de seguridad para la interoperabilidad de sistemas FTS: Etiquetado de seguridad y filtrado.

Para refinar la arquitectura de interoperabilidad de sistemas FTS, es esencial realizar experimentos en los que se identificaran la disponibilidad de los mismos y se mejorarán los componentes de seguridad requeridos, para permitir un flexible y seguro intercambio de datos desde los distintos sistemas FTS, en un entorno multi-nivel de seguridad y en un escenario multi-nacional.

Este requerimiento de seguridad no es específico para la interoperabilidad de los sistemas FTS, la interoperabilidad de sistemas FTS se tomará como caso de estudio para la implementación de soluciones de seguridad más genéricas.

Se requiere una aproximación incremental, partiendo de la situación actual, para reducir la complejidad y el riesgo de los futuros desarrollos. Actualmente, el escenario más relevante, en términos de seguridad, que se puede plantear en interoperabilidad de sistemas FTS es el intercambio bi-direccional de información entre sistemas nacionales FTS a nivel restringido y/o secreto.

3. Proceso de transferencia de datos mejorado: Compresión de datos.

La elección de XML [86] para la definición de los mensajes NFFI trae consigo ventajas, aunque también hay que tener en cuenta posibles ineficiencias a la hora de comprimir los datos debido al uso de XML.

La implementación de la actual arquitectura de interoperabilidad tiene en cuenta estas posibles ineficiencias, sin embargo, el ancho de banda de las comunicaciones siempre es un recurso escaso en el espacio de operaciones, es este sentido una reducción de este requerimiento, gracias a una mayor compresión de los datos, es muy positiva ya que permite reservar ancho de banda para comunicaciones más prioritarias.

Si el ratio de compresión es elevado, la arquitectura de interoperabilidad podría ser extendida muy cerca del espacio de operaciones al utilizar un menor ancho de banda.

Una mejora o revisión de la definición del estándar NFFI v1.3 es necesaria, aunque dadas las actividades que se están llevando a cabo en paralelo en el proceso final de estandarización del NFFI, se ha decidido que la mejora o revisión del NFFI no sea un tema prioritario para esta demostración, la cual se centrará principalmente en los aspectos mencionados en los párrafos anteriores.

#### 4.4.4.3 Países y sistemas participantes en la demostración CWID 2007

La lista que se muestra en la tabla 10 recoge las naciones, empresas o agencias OTAN que han participado en el ejercicio NBFSA-III durante la demostración CWID 2007.

Se puede dividir a los sistemas participantes dentro de tres grupos o roles: “Producer” (P) o sistemas que facilitan datos a otros sistemas. “Consumer” (C) o sistemas FFT que solo reciben datos desde otros sistemas FFT. “Enable” (E) o sistemas que facilitan otras capacidades.

Nación	Sistema/Trial	Organización	Role
DINAMARCA	DNK Navy Trial	Terma	C
DINAMARCA	ADD-CT Trial	Terma	C
FRANCIA	SIR / BFT-Imp@act	MOD / EADS-France	P, C
FRANCIA	SICF	MOD / Thales Group	C
FRANCIA	T-BMS / Maestro	MOD / Thales Group	P, C
ALEMANIA	Army CCIS	MOD / EADS-Germany	P, C
GRAN BRETAÑA	Co-JOP Trial	Fujitsu	C
ITALIA	SIACCOM (BFSA)	MOD / Selex Communications	C
ITALIA	IT-BFT	IT Army Intel & Signal HQ	P, C
OTAN	ACCS	NACMA	C
OTAN	LTIS/NBFSA	NATO C3 Agency (NC3A)	P, C
OTAN	JCOP (TBD)	NATO C3 Agency (NC3A)	C
OTAN	NFFI GY/JCHAT Trial	NATO C3 Agency (NC3A)	P
OTAN	IEG (TBD)	NATO C3 Agency (NC3A)	E
OTAN	X-GUARD	NATO C3 Agency (NC3A)	E
NORUEGA	NORCCIS (BFT)	NOR Defense Logistic Org.	P, C
NORUEGA	SOA	FFI	E
RUMANIA	SIAAB	MOD / Contractors	P, C
RUMANIA	SICIB	MOD / Contractors	C
ESPAÑA	SIMACOP	MOD / Contractors	P, C

**Tabla 10 Países y sistemas participantes en la demostración CWID 2007**

El papel de la NC3A en el CWID 2007 es triple:

- Líder de la demostración y facilita una estructura común para desarrollar los diferentes ejercicios y demostraciones de la OTAN.
- Coordinador y supervisor de las especificaciones del interfaz.
- Desarrollador de prototipos de sistemas Producers, Consumers y Enable.

#### **4.4.4.4 Fases de la demostración internacional CWID 2007**

La demostración internacional CWID 2007 consta de las siguientes fases:

1. Actividades Pre-CWID 07:
  - Formulación de un Trial Definition Plan (TDP) [87] consensuado.
  - Especificación de los interfaces acordados (extensiones del estándar NFFI versión 1.3)
  - Implementación tanto de la parte cliente como de la parte de servicios en cada sistema participante en la demostración.
  - Pre-pruebas de todo lo expuesto anteriormente (remotas)
2. Actividades durante la demostración CWID 07
  - Experimentos debidos
  - Evaluación inicial de los resultados
3. Actividades Post-CWID 07
  - Evaluación completa de los resultados de los experimentos realizados
  - Identificación y definición de los cambios requeridos en las especificaciones del interfaz.
  - Consolidación de los cambios software

Uno de los resultados esperados de los experimentos es la contribución a la mejora y extensión de la especificación NFFI.

#### **4.4.4.5 Especificación del interfaz utilizado en los experimentos del CWID 07**

Formato de los datos intercambiados:

El formato de los datos que se intercambiarán durante los experimentos no es el principal objetivo de la demostración, ya que todos siguen la definición NFFI actual. Sin embargo algunos experimentos pueden buscar la validación del uso de algunas secciones de datos del mensaje NFFI, cuyo uso no ha sido probado anteriormente en experimentos con sistemas FTS reales.

### Perfiles de los servicios de interoperabilidad:

Los perfiles de los servicios de interoperabilidad o Service Interoperability Profiles (SIP's), describen el aspecto funcional del interfaz utilizado durante la demostración. SIP es el actual nombre para los protocolos de interfaz o Interface Protocols o Interface Profile, (abreviados como "IP").

Esta nomenclatura puede plantear ambigüedades con otros significados de las siglas IP como por ejemplo, Internet Protocol, por esta razón se hace esta aclaración en este punto de este apartado y de esta forma evitar posibles confusiones, ya que los SIP's que existen actualmente han sido llamados IP1, IP2 e IP3 respectivamente.

Los SIP's que están actualmente incluidos en el estándar NFFI (IP1 e IP2), no van a ser revisados en profundidad durante el ejercicio NBFSA-III y por tanto no son un objetivo principal de la demostración CWID 2007.

Sin embargo, uno de los principales objetivos del ejercicio NBFSA-III es la revisión, mejora y extensión del SIP IP3, que fue definido y parcialmente probado durante la demostración CWID 2006 y más tarde no fue incluido en el estándar NFFI, durante la demostración CWID 2007 se ha definido un nuevo SIP, como extensión del ya mencionado IP3.

El nuevo IP3 es un SIP para un servidor de seguimiento de fuerzas, este SIP soporta las peticiones de los clientes sobre datos actualizados y/o históricos, así como la suscripción a nuevas actualizaciones de datos. La especificación de este interfaz es compatible con los servicios de interoperabilidad Web o Web Services Interoperability (WS-I) Basic Profile version 1.1.

La implementación de este SIP puede ser bastante más compleja la de los IP1, IP2 y la antigua versión del propio IP3. La implementación de las completas funcionalidades del nuevo IP3 [88] ha sido dividida en tres niveles funcionales:

- IP3 - FL1: Interacción Request-Response (síncrona), con capacidades básicas de realizar requerimientos de datos.
- IP3 – FL2: Extensión del FL1 para incluir una capacidad mayor de realizar requerimientos de datos. Además de la interacción Request-Response síncrona, el FL2 soporta también una funcionalidad de envío de datos "push" asíncrona con una funcionalidad de filtrado y requerimientos de datos limitada.
- IP3 – FL3: Extensiones de las funcionalidades del FL2, en particular la funcionalidad de filtrado y requerimientos de datos.

Durante el desarrollo de la demostración CWID 2007, uno de los principales objetivos será probar la viabilidad del SIP IP3-FL2, ya que el IP-FL1 fue probado, aunque no con mucha profundidad, durante la demostración CWID 2006.

En lo que se refiere al IP3-FL3, las expectativas son llevar a cabo con éxito algunas pruebas experimentales entre los países participantes en la demostración, para consolidar y validar, en la medida de lo posible, su especificación.

#### 4.4.4.6 Configuración del sistema de la demostración CWID 2007

La figura 68 recoge la configuración global de la demostración CWID 2007, en esta figura se pueden ver todos los sistemas operacionales o prototipos experimentales mostrados en la tabla 10.

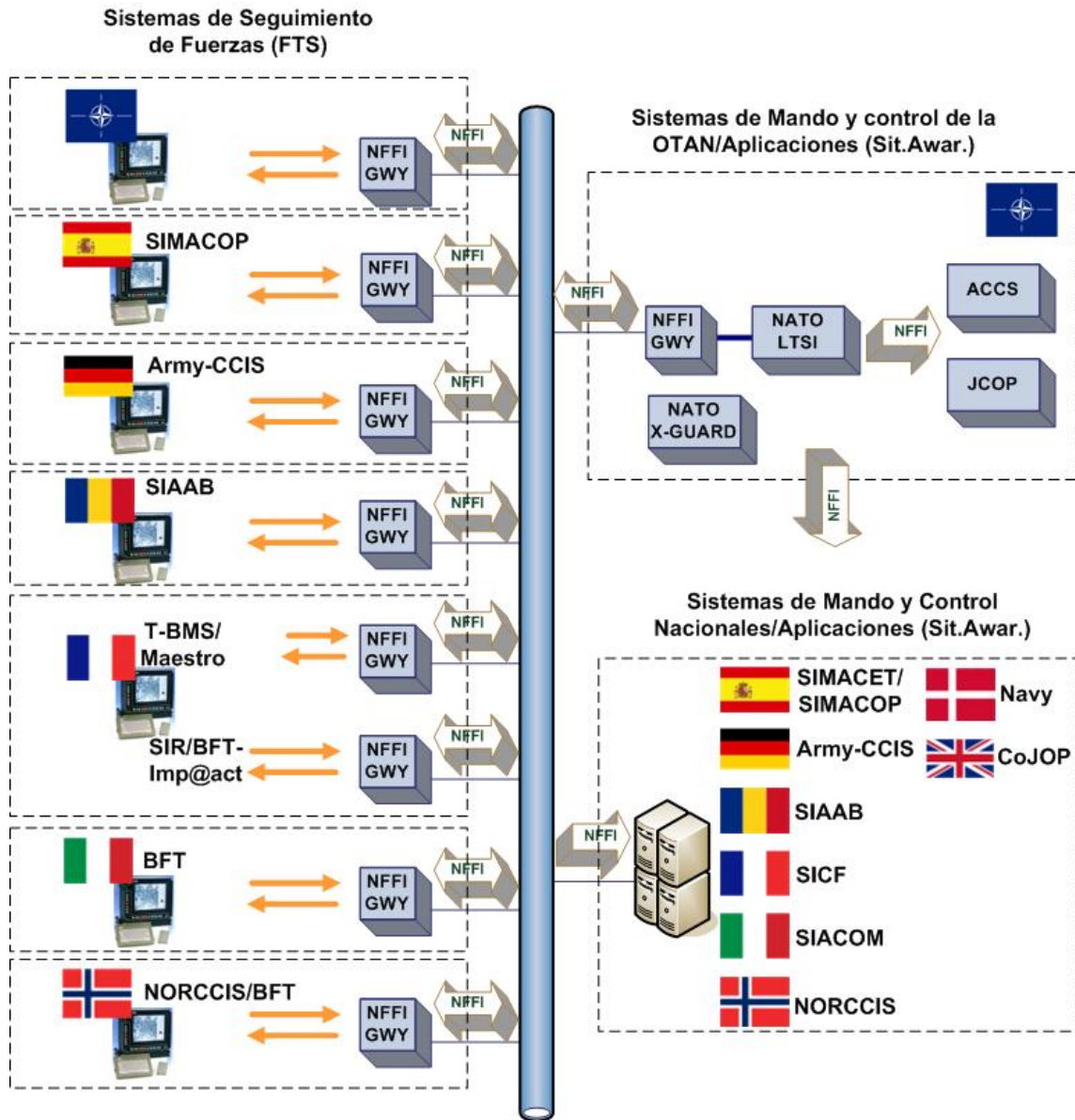


Figura 68

La demostración se llevará a cabo en un solo dominio de seguridad (simulado SECRETO).

Los subsistemas y componentes mostrados en la figura 68 son los siguientes:

- Sistemas FTS representan los sistemas tácticos de tierra y/o subsistemas de seguimiento de fuerzas amigas de las naciones participantes.

- Los sistemas FTS participantes serán los proveedores de los datos de seguimiento de las fuerzas propias de cada nación.
- NATO/National NFFI Gateway, representa el interfaz entre un sistema nacional FTS y la red NFFI, dentro de este interfaz se incluye soporte para el SIP “público” NFFI.
- Los sistemas de mando, control e información nacionales (C2IS) y los C2IS y aplicaciones relacionadas con el conocimiento de la situación o Situation Awareness (SA) de la OTAN, actuarán como Consumers de datos de seguimientos de fuerzas.
- El servidor de interoperabilidad de datos de seguimiento terrestres o NATO Land Tracks Interoperability Server (LTIS), representa el componente OTAN responsable de la gestión de los sistemas FTS’s de la OTAN y de la recolección, reparto y solución de conflictos relacionados con los datos de seguimientos, originados por cualquier sistema FTS participante.
- El componente NATO X-Guard (XML Guard), es un dispositivo de protección de frontera, permite el intercambio bidireccional de datos a través de dos dominios diferentes, reforzando la confianza y seguridad de las transmisiones de acuerdo con los niveles de seguridad de los datos.

#### 4.4.4.7 Evaluación de los resultados

Unas métricas comunes, estandarizadas y fácilmente aplicables han sido seleccionadas para llevar a cabo la evaluación de las pruebas realizadas por cada participante en la demostración CWID 2007.

En términos generales los resultados de cada participante se evaluarán teniendo en cuenta los siguientes datos:

Disponibilidad de los Datos/Información o Data Availability (DA) y la calidad de dichos Datos/Información o Data Quality (DQ). En este sentido se han introducido un limitado número de medidas de desarrollo o Measures of Performance (MoP), comunes para medir variables elementales que representan la DA y la QA para todas las pruebas llevadas a cabo durante la demostración. Cada MoP puede ser aplicable o no, dependiendo del tipo de experimento.

La descripción de las distintas MoP se muestra en la tabla 11.

<b>Codigo</b>	<b>Nombre</b>	<b>Significado</b>	<b>Valores</b>
MoP1	Número de seguimiento correcto	Cada dato de seguimiento enviado es recibido por sus receptores	Booleano (SI/NO)
MoP2	Formato de los datos correcto	El dato de seguimiento recibido por el receptor esta en formato NFFI correcto.	Boolean (SI/NO)
MoP3	Datos semánticas correctos	La semántica de los datos de seguimiento recibidos por el receptor son los mismos que los utilizados por el transmisor, por ejemplo; posición, DTG.	Booleano (SI/NO)
MoP4	Visualización correcta de los datos	Los seguimientos son correctamente visualizados en la pantalla de situación del receptor, por ejemplo; localización, símbolos gráficos.	Booleano (SI/NO)
MoP5	Filtrado correcto de los datos	Únicamente los datos permitidos, de acuerdo a la clasificación de seguridad del experimento, se transmiten desde el transmisor hasta el receptor de los datos.	Booleano (SI/NO)
MoP6	Latencia	Medida de la latencia introducido por los dispositivos que participan en el experimento	Segundos
MoP7	Ratio de compresión	El valor numérico del tamaño de los datos originales dividido por el tamaño de los datos recibidos.	Número

**Tabla 11 Lista de medidas de desarrollo o Measures of Performance (MoP)**

Se utilizarán también procedimientos comunes para llevar a cabo las medidas, con objeto de lograr una consistencia en la medida de las MoP de cada experimento. El éxito o el fracaso de cada experimento vendrán dados por la comparación entre las MoP medidas durante el experimento y los valores esperados de las mismas.



#### 4.4.4.8 Descripción de los experimentos

Todos los experimentos que se han realizado en la demostración CWID 2007, se han agrupado en cuatro grandes grupos, en base a las funcionalidades que se van a probar en cada experimento. Estos cuatro grupos de experimentos con sus MoP aplicables se muestran en la tabla 12.

Experimentos			MoPs						
Código	Título	Descripción	1	2	3	4	5	6	7
TS1	WS-Interfaz	Pruebas de los Producers y Consumers sobre el interfaz IP3							
1.A		Nivel funcional 1 (FL1)	S	S	S	S			
1.B		Nivel funcional 2 (FL2)	S	S	S	S			
1.C		Nivel funcional 3 (FL3)	S	S	S	S			
TS2	Compresión	Pruebas sobre compresión de datos							
2.A.1		Algoritmo-1: EFX. IP1	S	S	S				S
2.A.2		Algoritmo -1: EFX. IP3	S	S	S				S
2.B.1		Algoritmo -2: ALGX. IP1	S	S	S				S
2.B.2		Algoritmo -2: ALGX. IP3	S	S	S				S
2.C		Compresión a través de dominios	S	S	S			S	S
TS3	Seguridad	Distintas pruebas sobre seguridad							
3.A.1		Etiquetado/Filtrado con etiquetado externo	S	S	S		S		
3.A.2		Etiquetado/Filtrado con etiquetado interno	S	S	S		S		
3.B		[SOAP Seguridad] – IP3							
3.C		Otras pruebas de seguridad							
TS4	Miscellaneous	Pruebas adicionales sobre IP1/IP2 y DEF							
4.A		Pruebas Basicas/Avanzadas sobre IP1/IP2							
4.B		Pruebas avanzadas sobre DEF							
4.C		Pruebas de estrés							

**Tabla 12 Listado de experimentos de la demostración CWID 2007**

Los experimentos específicos de cada grupo de experimentos, en los que participe el sistema SIMACOP, se describirán con más detalle en el siguiente apartado de la presente tesis doctoral.

#### 4.4.4.9 Descripción detallada de las pruebas realizadas al sistema SIMACOP

La descripción detallada de cada uno de los experimentos en los que ha participado el sistema SIMACOP se muestra en las siguientes tablas;

<b>ID de la prueba</b>	403
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	RO - SIAAB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p>

	<p>Nombre MoP4  Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida) Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>
<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	RO - SICIB

**Tabla 13 Descripción del experimento 403**

<b>ID de la prueba</b>	405
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	RO - SICIB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida) Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	RO - SICIB

**Tabla 14 Descripción del experimento 405**

<b>ID de la prueba</b>	409
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	RO - SICIB SP - SIMACOP
<b>Tipo de mensaje</b>	
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida) Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	RO - SICIB
<b>Nombre del sistema consumidor de datos</b>	SP - SIMACOP

**Tabla 15 Descripción del experimento 409**

<b>ID de la prueba</b>	411
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	RO - SICIB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>



<b>Nombre del sistema proveedor de datos</b>	RO - SICIB
<b>Nombre del sistema consumidor de datos</b>	SP - SIMACOP

**Tabla 16 Descripción del experimento 411**

<b>ID de la prueba</b>	460
<b>Descripción</b>	Cuando algún video es considerado de interés a nivel operacional debería ser enviado y puesto a disposición de los usuarios de alto nivel del sistema. De esta forma el video estaría disponible para estos usuarios en forma de una etiqueta georeferenciada.
<b>Sistemas participantes en la prueba</b>	SP – COP SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	N/A
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	FTP
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Cuando en el nivel táctico se presume que algún video capturado es de relevancia para el nivel superior se envían los ficheros al SIOPERFAS-COP.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Comprobar que los videos se reciben correctamente georeferenciados.
<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	SP - COP

**Tabla 17 Descripción del experimento 460**

<b>ID de la prueba</b>	480
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFT SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	IT - BFT

**Tabla 18 Descripción del experimento 480**

<b>ID de la prueba</b>	482
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFT SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI, Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	IT - BFT

**Tabla 19 Descripción del experimento 482**

<b>ID de la prueba</b>	484
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFT SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida), Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	IT - BFT
<b>Nombre del sistema consumidor de datos</b>	SP - SIMACOP

**Tabla 20 Descripción del experimento 484**



<b>ID de la prueba</b>	485
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFT SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario, Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	IT - BFT

**Tabla 21 Descripción del experimento 485**

<b>ID de la prueba</b>	531
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFSA SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario, Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI, Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	IT - BFSA
<b>Nombre del sistema consumidor de datos</b>	SP - SIMACOP

**Tabla 22 Descripción del experimento 531**

<b>ID de la prueba</b>	532
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFSA SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero</b>	
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida) Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	IT - BFSA
<b>Nombre del sistema consumidor de datos</b>	SP - SIMACOP

**Tabla 23 Descripción del experimento 532**

<b>ID de la prueba</b>	639
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	IT – BFSA SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket TCP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	IT - BFSA

**Tabla 24 Descripción del experimento 639**



<b>IDde la prueba</b>	640
<b>Descripción</b>	<p>Grupo TS4 - Apartado 2 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP2 como protocolo de interfaz basado en UDP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados.</p>
<b>Sistemas participantes en la prueba</b>	IT - BFSA SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	UDP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de datos de seguimiento (en formato XML) a través de un socket UDP
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Cada dato de seguimiento enviado es recibido por su destinatario. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	SP - SIMACOP
<b>Nombre del sistema consumidor de datos</b>	IT - BFSA

**Tabla 25 Descripción del experimento 640**

<b>ID de la prueba</b>	1512
<b>Descripción</b>	<p>Grupo TS4 - Apartado 2 –  Prueba del interfaz de servicio Web IP3 a nivel funcional 1 (petición/respuesta, sin filtrado).  Los participantes implementarán el interfaz IP3 almacenando los datos de la prueba, también implementará un mecanismo para generar nuevos datos (inyector).  Este servidor será interrogado por los clientes IP3 usando diferentes combinaciones de los parámetros de llamada.  El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS.  No se implementara ningún tipo de filtrado, historyDepth=1</p>
<b>Sistemas participantes en la prueba</b>	DK - ADD-COIN DK - C4I C-Flex FR - TBMS IT - BFS A IT - BFT NATO - ACCS LOC1 NATO - NBFS A-III NO - BFS A/NFFI RO - SICIB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	SOAP
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	1. Se acuerdan los puntos finales de servicio. 2. Se acuerdan los parámetros de las consultas 3. Se confirma que el servicio está activo.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos. Valor Booleano (Si/No) Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI Valor Booleano (Si/No)

	<p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida) Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>
<b>Nombre del sistema proveedor de datos</b>	FR-BFT
<b>Nombre del sistema consumidor de datos</b>	NATO - NBFA-III

**Tabla 26 Descripción del experimento 1512**

<b>ID de la prueba</b>	1513
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 –</p> <p>El objetivo de la prueba es validar las especificaciones IP1/IP2.</p> <p>El proveedor de datos (iniciador del test) soportará los SIP's IP1 e IP2 y podrá generar datos o reenviar paquetes NFFI. El receptor de los datos ha de soportar los mismos SIP's.</p> <p>Los proveedores de datos enviarán datos usando IP1 e IP2 y variando la configuración de los datos.</p> <p>El Rx recibe los datos y mide los resultados del test.</p>
<b>Sistemas participantes en la prueba</b>	<p>IT - BFSa</p> <p>IT - BFT</p> <p>NATO - NBFSa-III</p> <p>NO - BFSa/NFFI</p> <p>RO - SIAAB</p> <p>SP - SIMACOP</p>
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero</b>	.xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	<p>1. Se acuerdan la dirección IP y el número de los puertos del receptor.</p> <p>2. Se confirma que el servicio está activo en el lado del receptor.</p>
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1</p> <p>Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos.</p> <p>Valor Booleano (Si/No)</p> <p>Nombre MoP2</p> <p>Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3</p> <p>Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor.. Valor Booleano (Si/No)</p> <p>Nombre MoP4</p> <p>Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida)</p> <p>Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	FR-BFT
<b>Nombre del sistema consumidor de datos</b>	RO-SICIB

**Tabla 27 Descripción del experimento 1513**

<b>ID de la prueba</b>	1542
<b>Descripción</b>	<p>Grupo TS4 - Apartado 2 – Servicio Web IP3  Prueba a nivel funcional 1.  (petición/respuesta, sin filtrado).  Los participantes implementarán el interfaz IP3 almacenando los datos de la prueba, también implementará un mecanismo para generar nuevos datos (inyector). Este servidor será interrogado por los clientes IP3 usando diferentes combinaciones de los parámetros de llamada. El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS.</p>
<b>Sistemas participantes en la prueba</b>	DK - ADD-COIN DK - C4I C-Flex FR - BFT FR - TBMS GE - Army CCIS IT - BFS A IT - BFT NATO - ACCS LOC1 NATO - JCOP NATO - NBFSA-III NO - BFS A/NFFI RO - SICIB SP - SIMACOP UK - CoJOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de los datos de seguimientos a través de un socket TCP.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos. Valor Booleano (Si/No) Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)

	<p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>
<b>Nombre del sistema proveedor de datos</b>	FR - TBMS

**Tabla 28 Descripción del experimento 1542**



<b>ID de la prueba</b>	1549
<b>Descripción</b>	<p>Grupo TS4 - Apartado 2 – Servicio Web IP3  Prueba a nivel funcional 1.  (petición/respuesta, sin filtrado).  Cada participante en la prueba implementará el interfaz IP3 como servidor almacenando los datos de la prueba, también implementará un mecanismo para generar nuevos datos (inyector). Este servidor será interrogado por los clientes IP3 usando diferentes combinaciones de los parámetros de llamada.  El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS.</p>
<b>Sistemas participantes en la prueba</b>	DK - ADD-COIN DK - C4I C-Flex FR - BFT FR - SICF FR - SIR GE - Army CCIS IT - BFS A IT - BFT NATO - ACCS LOC1 NATO - JCOP NATO - NBFS A-III NO - BFS A/NFFI RO - SICIB SP - SIMACOP UK - CoJOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envió de los datos de seguimientos (en formato xml) a través de un socket TCP.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos. Valor Booleano (Si/No)

	<p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>
<b>Nombre del sistema proveedor de datos</b>	FR - SICF

**Tabla 29 Descripción del experimento 1549**

<b>ID de la prueba</b>	1558
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 – Interoperabilidad horizontal. Intercambio de datos de seguimientos entre sistemas productores de seguimientos (FTS).</p> <p>Los participantotes (Producers) intercambian/comparten datos de seguimientos en formato NFFI utilizando streaming unicast fiable (push) e IP1 como protocolo de interfaz basado en TCP. Se probarán diferentes parámetros de intercambio de datos y diferentes combinaciones de los mismos.</p> <p>El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS. Esto es necesario tanto para la evaluación de los resultados como por motivos de presentación. Se usarán datos simulados durante la prueba.</p>
<b>Sistemas participantes en la prueba</b>	FR - BFT FR - SIR FR - TBMS NATO - NBFSA-III NO - BFSA/NFFI SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	N/A
<b>Protocolo de aplicación</b>	N/A
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	Envío de los datos de seguimientos (en formato xml) a través de un socket TCP.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos. Valor Booleano (Si/No) Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No) Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)

	Nombre MoP7 Ratio de compresión  Se considera éxito si de MoP1 a MoP3=Si y MoP7>10
<b>Nombre del sistema proveedor de datos</b>	FR - TBMS

**Tabla 30 Descripción del experimento 1558**

<b>ID de la prueba</b>	1568
<b>Descripción</b>	<p>Grupo TS4 - Apartado 2 –  Prueba del interfaz de servicio Web IP3 a nivel funcional 1 (petición/respuesta, sin filtrado).  Los participantes implementarán el interfaz IP3 almacenando los datos de la prueba, también implementará un mecanismo para generar nuevos datos (inyector). Este servidor será interrogado por los clientes IP3 usando diferentes combinaciones de los parámetros de llamada. El resultado del intercambio (datos recibidos en el sistema consumidor) se visualizarán en una aplicación de conocimiento de la situación asociada a cada sistema FTS.</p>
<b>Sistemas participantes en la prueba</b>	DK - ADD-COIN DK - C4I C-Flex FR - BFT FR - SICF FR - TBMS IT - BFS A NATO - ACCS LOC1 NATO - NBFSA-III NO - BFS A/NFFI RO - SIAAB RO - SICIB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	SOAP
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	1. Se acuerdan los puntos finales de servicio. 2. Se acuerdan los parámetros de las consultas 3. Se confirma que el servicio está activo.
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	Métricas de los resultados (MoP) Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios correctos. Valor Booleano (Si/No) Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI. Valor Booleano (Si/No)

	<p>Nombre MoP3  Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición.  Valor Booleano (Si/No)</p> <p>Nombre MoP4  Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>
<b>Nombre del sistema proveedor de datos</b>	RO - SIAAB

**Tabla 31 Descripción del experimento 1568**

<b>ID de la prueba</b>	1587
<b>Descripción</b>	<p>Grupo TS4 - Apartado 1 –</p> <p>El objetivo de la prueba es validar las especificaciones IP1/IP2.</p> <p>El proveedor de datos (iniciador del test) soportará los SIP's IP1 e IP2 y podrá generar datos o reenviar paquetes NFFI. El receptor de los datos ha de soportar los mismos SIP's.</p> <p>Los proveedores de datos enviarán datos usando IP1 e IP2 y variando la configuración de los datos.</p> <p>El receptor recibe los datos y mide los resultados de la prueba.</p>
<b>Sistemas participantes en la prueba</b>	RO - SIAAB SP - SIMACOP
<b>Tipo de mensaje</b>	N/A
<b>Formato del mensaje</b>	NFFI
<b>Formato de fichero (tipo MIME)</b>	.xml
<b>Protocolo de aplicación</b>	SOAP
<b>Protocolo de nivel de transporte</b>	TCP / IP v4
<b>Proceso de inicio. ¿Cuales son los procedimientos para iniciar la prueba?</b>	<ol style="list-style-type: none"> <li>1. Se acuerdan la dirección IP y el número de los puertos del receptor..</li> <li>2. Se confirma que el servicio está activo en el lado del receptor.</li> </ol>
<b>Proceso de Verificación. ¿Qué métricas probarán que la prueba a tenido éxito?</b>	<p>Métricas de los resultados (MoP)</p> <p>Nombre MoP1 Significado: Número de secuencia correcto, cada dato enviado es recibido por sus destinatarios. Valor Booleano (Si/No)</p> <p>Nombre MoP2 Significado: Los datos recibidos por el destinatario están en correcto formato NFFI Valor Booleano (Si/No)</p> <p>Nombre MoP3 Significado: la semántica de los datos recibidos por el destinatario (en su formato nativo) es la misma que la usada por el transmisor, por ejemplo, posición. Valor Booleano (Si/No)</p> <p>Nombre MoP4 Significado: los datos recibidos se visualizan correctamente en la pantalla de situación del receptor (localización, símbolo de la unidad seguida). Valor Booleano (Si/No)</p> <p>Se considera éxito si de MoP1 a MoP4=Si</p>

<b>Nombre del sistema proveedor de datos</b>	RO SIAAB
<b>Nombre del sistema consumidor de datos</b>	SP SIMACOP

**Tabla 32 Descripción del experimento 1587**



#### 4.4.5 Evaluación de SIMACOP en su demostración en el CWID internacional 2007

En la tabla 33 se pueden ver los resultados de las diferentes métricas utilizadas para validar el resultado de cada prueba realizada durante la demostración internacional CWID 2007, así como el resultado final de cada una de ellas.

Prueba ID	MoP1	MoP2	MoP3	MoP4	MoP7	RESULTADO
403	SI	SI	SI	SI	NA	EXITO
405	SI	SI	SI	SI	NA	EXITO
409	SI	SI	SI	SI	NA	EXITO
411	SI	SI	SI	SI	NA	EXITO
460	NA	NA	NA	SI	NA	EXITO
480	SI	SI	SI	SI	NA	EXITO
482	SI	SI	SI	SI	NA	EXITO
484	SI	SI	SI	SI	NA	EXITO
485	SI	SI	SI	SI	NA	EXITO
531	SI	SI	SI	SI	NA	EXITO
532	SI	SI	SI	SI	NA	EXITO
539	SI	SI	SI	SI	NA	EXITO
640	SI	SI	SI	SI	NA	EXITO
1512	SI	SI	SI	SI	NA	EXITO
1513	SI	SI	SI	SI	NA	EXITO
1542	SI	SI	SI	SI	NA	EXITO
1549	SI	SI	SI	SI	NA	EXITO
1558	SI	SI	SI	NA	SI	EXITO
1568	SI	SI	SI	SI	NA	EXITO
1587	SI	SI	SI	SI	NA	EXITO

**Tabla 33 Resumen de la evaluación de las pruebas en las que ha participado SIMACOP**

Durante los experimentos descritos anteriormente y cuya evaluación se muestra en este apartado, el sistema SIMACOP utilizó el modelo de datos propuesto en la presente tesis doctoral, como núcleo de su base de datos.

El resultado exitoso de todos y cada uno de los experimentos de interoperabilidad en los que participó el sistema, junto con otros sistemas pertenecientes a diferentes países, valida el modelo de datos utilizado en un entorno multinacional.

La validación del modelo de datos se fundamenta en las siguientes afirmaciones:

- La interoperabilidad con otros sistemas BFT ha sido completa y todas las pruebas en las que ha participado SIMACOP, han sido calificadas como exitosas en su evaluación.

- Los datos enviados y recibidos por SIMACOP no necesitaron ningún tipo de conversión ni traducción al usarse la base de datos intermedia propuesta en la presente tesis.

Las posiciones de las fuerzas amigas recibidas fueron almacenadas correctamente y pudieron visualizarse en la pantalla de SIMACOP, así como los videos georeferenciados a través del modelo de datos (Prueba 460). Este experimento se corresponde con la modificación de funcionalidad propuesta en modelo de datos en el apartado 3.5 de la presente tesis.





## 5 Conclusiones finales y trabajo futuro

### 5.1 Conclusiones finales

Durante el transcurso de las investigaciones realizadas, con objeto de llevar a cabo el completo desarrollo de la presente tesis doctoral, se han ido cumpliendo uno por uno, todos los objetivos que se habían propuesto al comienzo de esta investigación

En este apartado de conclusiones finales, se va a describir como se han ido cumpliendo todos los objetivos prioritarios de esta investigación, los cuales como ya se ha dicho previamente fueron fijados al comienzo de la misma, así como las lecciones que se pueden extraer de la consecución de estos objetivos y los posibles beneficios que esta investigación puede aportar a la sociedad.

Los objetivos prioritarios de la presente tesis, que se han cumplido durante el desarrollo de la misma son los siguientes:

- Se ha realizado un exhaustivo análisis del estado del arte del modelado de datos para sistemas C2I militares y también se han definido algunos conceptos clave relacionados con las técnicas y metodologías de modelado de datos existentes hoy en día.

En concreto se han analizado y comparado 10 modelos de datos tácticos distintos, desde el LC2IEDM v2 que se publicó en marzo del 2000 hasta el JC3IEDM edición 3.1 que se publicó en diciembre de 2006, cinco de los modelos analizados son versiones distintas del mismo modelo de datos (el C2IEDM v6.15), con este estudio se ha podido constatar las mejoras introducidas y la evolución de los principales modelos de datos tácticos en los últimos 7 años.

- Para complementar la investigación realizada se han implementado los esquemas físicos de dos de estos modelos, en concreto el C2IEDM v6.15c y el JC3IEDM Edición 3.0. Cada uno de estos modelos cuenta con más de 200 tablas (203 tablas el C2IEDM y 245 tablas el JC3IEDM), cuyas estructuras y funcionalidad dentro del modelo se han estudiado en profundidad, con objeto de adquirir un conocimiento profundo sobre este tipo de modelos de datos para poder llevar a cabo el principal objetivo de esta tesis doctoral, la adaptación de este tipo de modelos de datos a la gestión de emergencias civiles con resultados satisfactorios.
- Se han planteado escenarios de crisis civiles para profundizar en el estudio de los modos de coordinación y gestión de estas crisis, atendiendo principalmente a la resolución de los problemas de mando y control detectados, así como a la coordinación entre los diferentes cuerpos de seguridad o servicios de emergencias.
- También se ha hecho hincapié en como esta coordinación entre las diferentes entidades que intervienen en la resolución de la crisis, podría mejorarse con la inclusión de sistemas de detección, monitorización y seguimiento de las unidades desplegadas sobre el terreno, dotados de comunicaciones en tiempo real e interoperables entre sí.

En este sentido, también se han descrito algunas actuaciones erróneas, por parte de las autoridades al mando de la gestión de la crisis, en emergencias civiles reales, como el ataque a las torres gemelas el 11 de septiembre de 2001 o el tsunami de diciembre de 2004.

Estos errores que se han descrito, se podrían haber evitado contando con la información que este tipo de sistemas pueden proporcionar a los gestores de la crisis, para tomar las decisiones y ordenes que se enviarán a las unidades desplegadas sobre el terreno.

- Se han descrito, analizado e implementado dos de las soluciones de interoperabilidad más extendidas actualmente, estas dos soluciones de interoperabilidad describen los procesos operativos de intercambio de datos entre sistemas de mando y control o C2IS la primera de ellas y entre los sistemas de seguimiento de fuerzas amigas o FFTS, la segunda de ellas.

La primera de las soluciones de interoperabilidad implementadas en la presente tesis, ha sido la solución de interoperabilidad de sistemas C2IS propuesta por el programa MIP (Multilateral Interoperability Program).

Esta solución consta de 3 partes principales; **una base de datos de gestión** del proceso de réplica (base de datos MIRD) entre los distintos interfaces de datos, los propios **interfaces de datos**, cuyos esquemas físicos son implementados como parte de las bases de datos de los sistemas de mando y control implicados en el proceso de réplica y una **pila de protocolos**, que deben implementar también todos los sistemas implicados en el proceso de réplica y que permiten llevar a cabo proceso de réplica automática entre los sistemas de mando y control o C2IS.

Los esquemas físicos de las bases de datos MIRD asociadas a los modelos de datos C2IEDM v6.15c y el JC3IEDM Edición 3.0, también fueron implementadas como parte de las investigaciones llevadas a cabo en la presente tesis. Estas bases de datos de gestión se pueden dividir conceptualmente en dos partes, la parte de gestión de la réplica y la parte dedicada a la gestión del interfaz de datos.

La segunda de las soluciones de interoperabilidad analizadas e implementadas durante la presente tesis, ha sido la solución basada en el uso del estándar NFFI versión 1.3, este estándar ha sido creado para facilitar la interoperabilidad de sistemas de seguimiento de fuerzas amigas o FFTS.

Esta solución define la estructura de los mensajes NFFI de manera que las informaciones de posicionamiento, además de otras informaciones relativas a las unidades seguidas por distintos sistemas FFTS, pueden ser intercambiadas entre ellos para tener una visión común del espacio de operaciones.

La compatibilidad o para ser rigurosos, el fácil mapeado, entre la información contenida en los mensajes NFFI y la información definida por el modelo C2IEDM diseñado por el programa MIP, ha sido también estudiado en profundidad en esta tesis, debido a la necesidad de mapear las informaciones de posicionamiento recibidas a través de mensajes NFFI en el interfaz de datos del sistema SIMACOP, que esta basado en el modelo C2IEDM.

Como resultado de las investigaciones realizadas, se ha propuesto y desarrollado un interfaz común de datos basado en el modelo C2IEDM v6.15c, para poder ser usado por las dos aplicaciones de interoperabilidad desarrolladas que se acaban de enunciar.

De esta forma se dota de la posibilidad de interoperar al sistema SIMACOP, propuesto por la presente tesis, como solución de sistemas de mando y control dedicados a la gestión de emergencias el ámbito civil, tanto con sistemas C2IS que implementen la solución MIP, como con sistemas FFTS que implementen la solución NFFI.

Dicha versatilidad a la hora de interoperar fue la principal razón que llevó a los mandos militares vinculados con el programa CWID, a proponer al sistema SIMACOP como sistema FFTS candidato para integrarse con el sistema de mando y control del ejército de tierra SIMACET.

La integración propuesta hacia uso de la aplicación de réplica basada en el estándar NFFI desarrollada en la presente tesis, para introducir en el modelo de datos MCD2ET 1.7 de SIMACET las posiciones de las fuerzas amigas propias, mapeadas directamente desde SIMCOP, como de otros países, que el sistema FFTS SIMACOP recibía a través de mensajes NFFI desde distintos sistemas FFTS de dichos países.

Para realizar la integración entre el interfaz de datos de SIMACOP, basado en el modelo C2IEDM y el modelo MCD2ET 1.7 de SIMACET se utilizó la herramienta de interconexión de sistemas Defense Information Infrastructure (DII) Common Operating Environment (COE).

- Se ha integrado el interfaz de datos desarrollado, así como las distintas aplicaciones de réplica de datos implementadas, dentro del sistema FFTS SIMACOP, que es el resultado del proyecto de investigación: TIN2004-03588-C4ISR Multimedia aplicado a la gestión de emergencias, financiado por el Ministerio de Ciencia y Tecnología y fondos FEDER, en el marco del cual se han llevado a cabo la mayoría de las investigaciones y desarrollos que componen esta tesis doctoral.

Se ha demostrado el correcto funcionamiento y viabilidad del prototipo del sistema SIMACOP y por ende de los desarrollos fruto de la presente tesis doctoral en pruebas oficiales del programa CWID, en concreto en la demostración nacional CWID 2006, realizada en la base de la brigada de transmisiones 21 del ejército en Marines (Valencia) y en la demostración internacional CWID 2007, realizada en las instalaciones de la OTAN en Jørstadmoen, Noruega.

Todos estos objetivos alcanzados y que se acaban de enumerar, se corresponden con los objetivos parciales enunciados en el apartado 1.2 de la presente tesis doctoral.

Por todo lo anteriormente expuesto, podemos decir que el desarrollo y la investigación que se han llevado a cabo durante esta tesis, se han ceñido a los objetivos fijados en el planteamiento inicial de la misma y que sus resultados se han probado en demostraciones oficiales y en condiciones reales con éxito.

En cuanto a las mejoras y ventajas, que las investigaciones realizadas en la presente tesis, pueden aportar en el campo de la resolución de emergencias civiles, podríamos enumerar las siguientes:

- La inclusión de sistemas de mando y control con interfaz de datos común para facilitar su interoperabilidad, como herramienta de gestión de crisis y apoyo a la coordinación de los distintos cuerpos de seguridad y servicios de emergencias encargados de acudir a la resolución de grandes crisis civiles.

El uso de este tipo de sistemas, conllevaría un notable incremento de la eficacia y coordinación de dichos cuerpos en sus actuaciones conjuntas durante el desarrollo de una crisis.

En primer lugar, este tipo de sistemas permitiría ofrecer a todos los actores al mando de la gestión de la crisis, una visión común operacional o Common Operational Picture (COP) del espacio de operaciones, los datos que el sistema mostraría en los nodos de nivel jerárquico más alto se recogerían directamente de los sensores incorporados a las distintas unidades desplegadas sobre el terreno. Estos sensores podrían ser desde video cámaras (diurnas o de infrarrojos), sensores biométricos, analizadores del aire, etc.

Se dispondría de esta forma en las escalas superiores del mando de video en tiempo real y de otras informaciones provenientes de las unidades, todos estos datos serían almacenados y replicados en tiempo real en las bases de datos de los distintos cuerpos de seguridad y servicios de emergencias encargados de la gestión de la crisis, lo que daría la visión común de la situación.

Además, estos sistemas de mando y control con estructura jerárquica contribuirían a aumentar la seguridad de los efectivos que se encuentran desplegados sobre el espacio de operaciones, ya que cada responsable tendría información a cerca de la posición y condiciones físicas de cada una de las unidades en cada momento.

De esta forma, se podrían tomar decisiones relacionadas con la concentración de efectivos, de una forma más óptima, allí donde la evolución de la crisis lo requiriera con más urgencia y a su vez, el disponer de información sobre la posición de las unidades, haría que se pudiera ayudar o evacuar, de una forma más rápida y por las unidades que se encuentren más próximas a ellas, a aquellas unidades que tengan problemas físicos y por lo tanto su integridad corra peligro.

Por otro lado, se podría informar directamente a las unidades de riesgos de posibles aislamientos, que puedan ponerlas en peligro. Un sistema de seguimiento de fuerzas sobre el terreno como el que se propone en estas conclusiones, hubiera podido detectar y posteriormente evitar, el aislamiento de la patrulla de voluntarios que quedó aislada por el fuego y luego pereció, en el incendio de Guadalajara del verano de 2005.

- El uso de un interfaz común de datos por parte de los distintos sistemas de las entidades encargadas de la gestión de la crisis, sería otra de las ventajas aportadas por la presente tesis doctoral.



De esta forma, las distintas entidades encargadas de la gestión de una crisis civil, tendrían una parte de las bases de datos de sus sistemas de mando y control que sería común a todas ellas y que permitiría el intercambio de información entre las diferentes agencias de forma automática.

A partir de poder compartir la misma información sobre la crisis, todos los mandos encargados de la gestión de la misma se facilitaría la coordinación y el uso adecuado de los recursos, que cada entidad tuviera que movilizar dentro del escenario de la crisis.

Con objeto de dar a conocer esta tecnología entre los diferentes cuerpos y servicios de emergencias, el Grupo de Sistemas de Tiempo Real Distribuidos de la Universidad Politécnica de Valencia esta trabajando conjuntamente con el cuerpo de bomberos de la ciudad de Valencia, dentro del marco del proyecto internacional MARIUS (Mobile Autonomous Reactive Information system for Urgency Situations) cofinanciado por la Comisión Europea.

El objetivo de este proyecto sería conseguir desarrollar un sistema de mando y control de despliegue rápido, que sea útil en la gestión y coordinación de crisis civiles a nivel europeo. Parte de las investigaciones que se han expuesto en la presente tesis también se han llevado a cabo dentro el marco del proyecto MARIUS.

Con todo lo expuesto hasta este momento, solo nos cabe insistir en la importancia de disponer, por parte de los responsables de la gestión de una crisis civil declarada, de información veraz y lo más actualizada y filtrada posible, que les permita tener una idea clara de lo que esta ocurriendo en el espacio de operaciones, para poder tomar con las máximas garantías las decisiones que conducirán a la resolución de dicha crisis, ya que en ella pueden estar involucradas un gran número de vidas humanas.

## **5.2 Trabajo futuro**

En este apartado se van a describir sucintamente las acciones a través de las cuales se van a continuar desarrollando las principales líneas de investigación que forman parte de la presente tesis doctoral

La continuidad de la línea de investigación sobre el modelado de datos para sistemas C2I para la gestión de emergencias está garantizada gracias al proyecto **TIN2007-67410** “Integración de redes de sensores en un sistema C4ISR multimedia para gestión de emergencias”, del plan nacional de I+D, que le ha sido concedido al grupo de Sistemas de Tiempo Real Distribuido de la UPV en el año 2007.

En este proyecto el objetivo principal es la definición de un arquitectura de sistema de tiempo real distribuido para este tipo de aplicaciones (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), teniendo como núcleo del sistema el modelo de datos C2IEDM modificado para gestión de emergencias civiles, y la integración de un número limitado de sensores multimedia, aplicados a los individuos involucrados en la gestión de la emergencia (bomberos, policía, protección civil): posicionamiento GPS, sensores biométricos y video streaming de alta calidad en tiempo real.

Los objetivos operacionales del proyecto se pueden resumir en los siguientes puntos:

1. Ampliar la arquitectura definida para integrar, tanto redes de sensores desplegables en caso de emergencia, como redes de sensores preexistentes en el entorno.
2. Definición de una nueva arquitectura de comunicaciones para la adecuada integración de las redes de sensores en el sistema C4ISR y la inclusión de las tecnologías de redes de datos inalámbrica WIMAX y UWB.
3. Explorar la idoneidad de integración de sistemas de ayuda a la decisión para este tipo de aplicaciones. Para ello, se tomará como base el sistema desarrollado en el anterior proyecto, aplicando en su ampliación la misma metodología de definición, implementación de un prototipo, validación de funcionalidades y evaluación de prestaciones.

Con la inclusión de nuevas funcionalidades como integración de redes de sensores y sistemas de ayuda a la decisión, el modelo de datos del nuevo sistema SIMCOP deberá ser actualizado y ampliado para poder seguir manteniendo las funcionalidades de interoperabilidad con las que ya contaba.

El sistema SIMACOP, que lleva integrado el modelo de datos desarrollado durante la elaboración de la presente tesis, participará activamente en las demostraciones finales de los siguientes proyectos internacionales pertenecientes al programa Preparatory Action for Security Resear (PASR), el cual está cofinanciado por la comisión europea.

**PASR-107900**-Mobile Autonomous Reactive Information system for Urgency Situations (MARIUS).

**PASR-SEC6-PR-204100-Common Intelligence and Traceability for Rescues and Identification Operations (CITRINE).**

Estas participaciones en las mencionadas demostraciones finales, permitirán nuevas evaluaciones del modelo de datos propuesto así como del sistema SIMACOP y constituirán un inmejorable banco de pruebas para las actualizaciones y mejoras que se introduzcan en un futuro próximo, tanto en el modelo de datos propuesto como en el propio sistema SIMACOP.

El programa PARS constituyó el embrión de la actual línea prioritaria de la Comisión Europea sobre seguridad, las próximas llamadas para la presentación de proyectos de investigación dentro de esta línea serán seguidas con especial interés por el grupo de investigación, con el fin de continuar las actividades realizadas en los proyectos mencionados.

Otra de las líneas de investigación, relacionada con la presente tesis doctoral, que va a continuar su desarrollo en el futuro, es la relacionada con la problemática de la interoperabilidad entre sistemas de mando y control y sistemas de seguimiento de fuerzas amigas (FFTS).

Concretamente se van a centrar las investigaciones en solucionar los problemas de interoperabilidad en este tipo de sistemas (FFTS), en tareas de gestión de emergencias civiles.

Para ello se continuará la investigación sobre el desarrollo y la evolución del estándar NFFI para facilitar y en la medida de lo posible estandarizar su aplicación, en el intercambio automático de información, entre sistemas FFTS dedicados a la gestión de emergencias civiles.

Por otro lado y continuando con la problemática de la interoperabilidad se continuara investigando sobre los nuevos desarrollos del programa MIP, concretamente el bloque 3, que ha comenzado su andadura en marzo de 2007.

Se implementarán versiones más estables del modelo J3CIEDM, ya que este modelo de datos se ha convertido recientemente en el NATO STANAG 5525, hemos de decir que este STANAG está actualmente pendiente de ratificación, la cual se espera antes de final del 2007.

De esta forma se van a poder actualizar y mejorar las aplicaciones de réplica desarrolladas durante la presente tesis y que permitan al sistema SIMACOP seguir interoperando en un futuro con el sistema de mando y control del ejército de tierra (SIMACET).

Todo lo dicho en esta tesis doctoral, hace que simplemente con una pequeña modificación en la frase que Marco Tulio Cicerón pronunciara hace más de 2000 años, esta frase pueda ser usada perfectamente para finalizar la presente tesis.

*“No basta con adquirir **información**, es preciso además saber usarla”.*



## 6 Referencias

---

- 1 Alberts, David S, Hayes, Richard E. Power to the Edge – Command and Control in the Information Age. Washington, D.C.: DoD Command and Control Research Program: June 2003
- 2 Jeffrey R. Doering, EVALUATION OF AN OBJECT-BASED DATA INTEROPERABILITY SOLUTION FOR AIR FORCE SYSTEMS, Submitted to the Department of Electrical of Electrical Engineering and Computer Science on May 22, 2000.
- 3 Natalia Andrienko and Gennady Andrienko, Intelligent Visualisation and Information Presentation for Civil Crisis Management, Fraunhofer Institute AIS, Sankt Augustin, Germany. Presented at 9th AGILE Conference on Geographic Information Science, Visegrád, Hungary, 2006
- 4 <http://www.mip-site.org>
- 5 Miguel y M. Piattini; Concepcion y diseño de bases de datos: del modelo E/R al modelo relacional. 1993
- 6 KORTH, Henry F. y SILBERSCHATZ, Abraham. (1993) Fundamentos de bases de datos. Madrid: McGraw-Hill
- 7 Peter P. Chen: The Entity-Relationship Model - Toward a Unified View of Data. (1976)
- 8 Batini, C., S. Ceri, S. Kant, and B. Navathe. Conceptual Database Design: An Entity Relational Approach. The Benjamin/Cummings Publishing Company, 1991.
- 9 Craig S. Mullins, Database Administration: The Complete Guide to Practices and Procedures. Publisher: Addison Wesley Professional, 2002
- 10 [http://www.mip-site.org/020\\_Public\\_History.htm#PA-Public-History-ATCCIS-02](http://www.mip-site.org/020_Public_History.htm#PA-Public-History-ATCCIS-02)
- 11 [http://www.mip-site.org/01-Atccis/ATCCIS\\_Home.htm](http://www.mip-site.org/01-Atccis/ATCCIS_Home.htm)
- 12 NATO ADatP-32, Edition 2.0: “The Land C2 Information Exchange Data Model“ NATO HQ, Brussels, March 2000
- 13 ATCCIS WORKING PAPER\_st\_02\_Main(Ed 2.0)\_31\_March\_2000
- 14 ATCCIS WORKING PAPER 14-3 (Ed 5.0)\_ 18\_March\_2002
- 15 NATO Corporate Data Model (STANAG 5523 / AdatP-32).
- 16 ATCCIS WORKING PAPER 5-7\_(Ed 5.0)\_18\_March\_2002
- 17 MTIDP-MIP\_Technical\_Interface\_Design\_Plan: MTIDP-SP-TWG-Edition1.4
- 18 ADatP-3 NATO Message Text Formatting System (FORMETS), Part I, System Concept and Description, Draft, 15 July 1993, NATO UNCLASSIFIED
- 19 MIP\_MTIDP\_ANNEXA\_DEM\_SPECIFICATION
- 20 NATO Policy on the Multilateral Interoperability Programme [NC3B AC/322-WP/0238]

- 
- 21 Multilateral Interoperability Program (MIP), 20 November 2003 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.1 (Unclassified)
  - 22 Multilateral Interoperability Program (MIP), 26 September 2004 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.15a (Unclassified)
  - 23 Multilateral Interoperability Program (MIP), 17 March 2005 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.15b (Unclassified)
  - 24 Multilateral Interoperability Program (MIP), 12 July 2005 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.15c (Unclassified)
  - 25 Multilateral Interoperability Program (MIP), 30 September 2005 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.15d (Unclassified)
  - 26 Multilateral Interoperability Program (MIP), 2 December 2005 “Command and Control Information Exchange Data Model”, (C2IEDM) Version 6.15e (Unclassified)
  - 27 MIP-NDAG-Memorandum of Agreement (MOA) 4 February 2004
  - 28 Multilateral Interoperability Program (MIP), 24 December 2004 “Joint C3 Information Exchange Data Model”, (JC3IEDM) edition 0.5 (Unclassified)
  - 29 Multilateral Interoperability Program (MIP), 9 December 2005 “Joint C3 Information Exchange Data Model”, (JC3IEDM) edition 3.0 (Unclassified)
  - 30 Standardisation agreement NATO: STANAG 5525: Joint Command, Control and Consultation Information Exchange Data Model, NATO UNCLASSIFIED, December 2005
  - 31 Multilateral Interoperability Program (MIP), 8 December 2006 “Joint C3 Information Exchange Data Model”, (JC3IEDM) edition 3.1 (Unclassified)
  - 32 Data Model Patterns: A Metadata Map, Autor David C. Hay, 2006 editorial; Morgan Kaufmann
  - 33 <http://www.edef.com/IDEF1X.html>
  - 34 NATO STANAG 2014 Formats for Orders and Designation of Timings, Locations and Boundaries
  - 35 <http://wwwn.mec.es/ciencia/personalTecnico/files/ProyectosID.pdf>
  - 36 [http://ec.europa.eu/enterprise/security/doc/project\\_flyers/766-06\\_marius.pdf](http://ec.europa.eu/enterprise/security/doc/project_flyers/766-06_marius.pdf)
  - 37 <http://www.dyvine.eu/>
  - 38 [http://www.9-11commission.gov/archive/hearing11/9-11Commission\\_Hearing\\_2004-05-19.htm](http://www.9-11commission.gov/archive/hearing11/9-11Commission_Hearing_2004-05-19.htm)
  - 39 [http://en.wikipedia.org/wiki/Humanitarian\\_response\\_to\\_the\\_2004\\_Indian\\_Ocean\\_earthquake](http://en.wikipedia.org/wiki/Humanitarian_response_to_the_2004_Indian_Ocean_earthquake)
  - 40 <http://www.embajadadeindonesia.es/contenido.asp?Id=6>
  - 41 <http://www.mysql.com>

- 
- 42 MIP TECHNICAL INTERFACE DESIGN PLAN (MTIDP) – SP – TWG 31, OCT 2003, Edition: 1.4
- 43 The NATO Policy for C3 Interoperability [NC3B Sub-Committee AC/322 SC/2-WP/72 (Revised) Version 4.3]: “Seamless Sharing of Information: Common Information Exchange.”
- 44 The NATO Policy for C3 Interoperability [NC3B Sub-Committee AC/322 SC/2-WP/72 (Revised) Version 4.3]: “Structured Data Exchange: Data Object Exchange”
- 45 STANAG 5048 - The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces (Edition 5. Promulgated 16 February 2000 by NC3B Sub-Committee AC/322 SC/1).
- 46 NATO Interoperability Planning Document (NIPD) “Level 5 of System Interconnection”
- 47 C2IEDM-MIRD-SP-MTIDPWP.Edition6.15c-2005-07-12.mdb
- 48 “Wireless LAN medium Access Control Protocol (MAC) and Physical Layer (PHY) Specification”, ANSI/IEEE Std 802.11:1999 (E) Part 11, ISO/IEC 880211, 1999
- 49 <http://www.nc3a.nato.int/>
- 50 STANAG 5527 NATO Friendly Force Information Standard for Interoperability of Force Tracking Systems
- 51 AC322(SC5)N(2006)0025 - Interim NFFI Standard for Interoperability of FTS, December 2006
- 52 NC3A, Hallingstad G., Porta R., April 2006 “Interoperability of Friendly Force Tracking Systems in Coalition Operations”, NC3A Technical Note 1182. (NATO Unclassified)
- 53 [US JBFSA ACTD], 12 June 2003 “Data Definition Specification – Joint Blue Force Situational Awareness (JBFSA) Message Translator to Radiant Mercury Interface”, Version 1.0. (Unclassified)
- 54 <http://www.military-information-technology.com/article.cfm?DocID=504>
- 55 NATO, Military Agency for Standardization (MAS), APP-6(A)/STANAG 2019, “Military Symbols for Land-Based Systems”, December 1999. (NATO Unclassified)
- 56 US Department of Defense, Interface Standard Common Warfighting Symbology; MIL-STD-2525A, 15 December 1996. (Unclassified – Limited Distribution)
- 57 NATO Standardization Organization STANAG 1059, edition 8, “Character Codes for Geographical Entities”, 19 February 2004. (NATO Unclassified)
- 58 <http://www.cwid.js.mil/c/extranet/home>
- 59 <http://www.defenselink.mil/>
- 60 W-Meilander, et.al. “Predictability for Real-Time Command and Control”. IEEE 2001.

- 
- 61 C4ISR Architecture Framework Versión 2.0. DoD Architectures Working Group. April, 1997.
- 62 B.T. Robinson. "Who goes there?". IEEE Spectrum. October, 2003.
- 63 R. Thomas, R.A. Beamer, P.K. Sowell. "Civilian Application of the DOD C4ISR Architecture Framework: A Treasure Department Case Study".
- 64 J.N. Martin, S.J. Heidorn. "Representing System Architectures using the C4ISR Architecture Framework". The Aerospace Corporation. March, 2002.
- 65 A. Meiser et al. "Design Challenges for an Integrated Disaster Management Communication and Information System". 1st IEEE Workshop on Disaster Recovery Networks. N.Y.C. June, 2002.
- 66 610.12 IEEE, standard glossary of software engineering terminology, Publication Date: 10 Dec 1990
- 67 M. Macpherson. "Embedded Solution Team", MITRE. May, 2000.
- 68 C.D. Gill et al. "Applying Adaptive Real-time Middleware to Address Grand Challenges of COTS-based Mission-Critical Real-Time Systems". 1st International Workshop on Real-Time Mission-Critical Systems. November, 1999.
- 69 J.A. Stankovic. Continuous and Multimedia OS Support In Real-Time Control Applications. In the Fifth Workshop on Hot Topics in Operating Systems (HotOS-V), pages 8-11, May 1995.
- 70 United States Federal Emergency Management Agency, available at <http://www.fema.gov>
- 71 C. Beard, "Mechanisms for Providing Internet Emergency Services", TR University of Missouri-Kansas City, Feb. 2003.
- 72 I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a Survey", Computer Networks, Vol. 38, pp.393-422, March 2002.
- 73 Specification of the Bluetooth System, Volumes 1 and 2, Core, Version 1.1. Bluetooth SIG, February 22 2001, <http://www.bluetooth.com>
- 74 C. E. Perkins, Ad Hoc Networking, Addison Wesley, 2001.
- 75 K. Ahmavaara, H. Haverinen and R. Pichna, "Integration of wireless LAN and 3G wireless – Interworking architecture between 3GPP and WLAN systems", IEEE Communications, v. 43, n. 11, pp. 74-81, Nov. 2003.
- 76 C. W. Bostian and S. F. Midkiff, "Demonstrating Rapidly Deployable Broadband Wireless Communications for Emergency Management," National Digital Government Research Conference, May 2002.
- 77 Steve Mann, "WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT" presented at the 1998 International Conference on Wearable Computing ICWC-98, Fairfax VA, May 1998
- 78 [http://www.ejercito.mde.es/organizacion/hqnrhc-sp/hq/mando\\_control.htm](http://www.ejercito.mde.es/organizacion/hqnrhc-sp/hq/mando_control.htm)



---

79 <http://www.ieee802.org/16/index.html> IEEE 802.16, Standard for Wireless Metropolitan Area Networks.

80 <http://www.isdefe.es/>

81 [http://www.sei.cmu.edu/str/descriptions/diicoe\\_body.html](http://www.sei.cmu.edu/str/descriptions/diicoe_body.html)

82 Defense Information Infrastructure (DII), Common Operating Environment (COE) Integration and Runtime Specification (I&RTS) version 3, 1 July 1997 (CM-400-01-04)

83 Ambrose Goicoechea, Ph.D. - Requirements, DII COE Compliance, and Multiple Criteria For Distributed Database Design - Software Engineering Center (SWEC), MITRE Corporation, 11493 Sunset Hills Road, Mail Stop W624, Reston, Virginia

84 NC3A (March 2006), NATO Friendly Force Tracking - CWID-06 Experimentation Report, NATO UNCLASSIFIED

85 NC3A (March 2006), NFFI version 1.2 – Interface Protocol Definition, IP3, Working Document (v 1.0), (NATO Unclassified)

86 <http://www.w3.org/XML/>

87 CWID-2007, NATO Blue Force Situation Awareness Trial Definition and Plan (v1.0), March 2007

88 NC3A (R. Malewicz) (March 2007), NFFI version 2.0 – Interface Protocol Definition, IP3, (NC3A working paper, work in progress), NATO UNCLASSIFIED