IDTRAM – Identificació i Detecció de Tramvia
Memòria

Autor : Pilar Morrón Anglès
Consultor: Oriol Martí Girona
Data de Lliurament : 9 de gener 2015

Copyright
© (l'autor/a)
Reservats tots els drets. Està prohibit la reproducció total o parcial d'aquesta obra per qualsevol mitjà o procediment, compresos la impressió, la reprografia, el microfilm, el tractament informàtic o qualsevol altre sistema, així com la distribució d'exemplars mitjançant lloguer i préstec, sense l'autorització escrita de l'autor o dels límits que autoritzi la Llei de Propietat Intel•lectual.

FITXA DEL TREBALL FINAL

Títol del treball:	*IDTRAM : Identificació i detecció de tramvies*
Nom de l'autor:	*Pilar Morrón Anglès*
Nom del consultor:	*Oriol Martí Girona*
Data de lliurament (mm/aaaa):	*09/01/2015*
Àrea del Treball Final:	*PFC- Adhoc*
Titulació:	*Enginyeria informàtica (2º cicle)*

Resum del Treball (màxim 250 paraules):

La necessitat creixent de garantir en les ciutats un mitja de transport respectuós amb el medi ambient, ha fet aparèixer de nou els tramvies com a alternativa silenciosa, còmoda, poc contaminant i ràpida, de transport públic sota un criteri de sostenibilitat en el entorn urbà. Per tal de reduir l'impacte estètic en zones monumentals o amb gran interès arquitectònic, els actuals sistemes de circulació sense cables comença a ser utilitzat de forma generalitzada en els tramvies que es troben en construcció o en tramvies ja construïts i que es volen ampliar.

Aquest treball final de carrera presenta l'anàlisi i disseny de un component software que forma part de un sistema de carrega sense catenària i que permet identificar i posicionar un tramvia sobre uns carrils conductors localitzats entre els carrils de rodadora amb el nivell de seguretat SIL 4 d'acord amb la norma EN 50128:2011 que afecta a tots els desenvolupaments software lligats al mon ferroviari.

El treball s'inicia amb l'arquitectura software del sistema que fa esment de tots els seus components per passar a centrar-se en la obtenció dels requisits i realització del disseny del component software objecte del treball. La metodologia utilitzada per la seva realització es basa en el model de disseny UML orientat a components basat en Rational Unified Process que aporta modularitat, ocultament de la informació o encapsulament que a mes a mes d'ajudar a controlar la complexitat del software, contribueix a millorar la seva mantenibilitat, verificació, validació i comprensió.

Índex

1 Introducció 3

1.1 Context i justificació del treball 3

1.2 Objectius del treball 4

1.3 Enfocament i mètode seguit 4

1.4 Planificació del treball 6

1.5 Breu sumari de productes obtinguts 7

1.6 Breu descripció d'altres capítols 9

2 Projecte 10

2.1 Descripció 10

2.2 Anàlisi de riscos 13

2.3 Gestió del projecte 14

2.4 Especificació de la arquitectura del sistema 16

2.5 Especificació de requisits del component IDTRAM 17

2.6 Especificació de proves de integració i sistema 18

2.7 Especificació de la arquitectura i disseny detallat del component IDTRAM 20

2.8 Registres de verificació 24

3 Conclusions 25

4 Glossari 26

5 Bibliografia 27

Llistat de Il·lustracions

Il·lustració 1 Estructura Organitzativa SIL4 6

Il·lustració 2 Planificació del projecte 7

Il·lustració 3 Composició del material mòbil 10

Il·lustració 4 Infraestructura de via 12

Il·lustració 5 Diagrama de components de la arquitectura software del sistema..... 16

Il·lustració 6 Entrades i sortides del procés pel disseny dels casos de prova..... 19

Il·lustració 7 Estructura del CSCI IDTRAM..... 22

Il·lustració 8 Diagrama de components del CSC IDT_MANAGER 23

Il·lustració 9 Diagrama de components del CSC IDT_COMMS..... 24

Llistat de Taules

Taula 1 Relació de productes obtinguts 9

Taula 2 Nivell de risc..... 13

Taula 3 Anàlisi de riscos 14

Taula 4 Registres de verificació 25

1 Introducció

1.1 Context i justificació del treball

El present treball final de carrera pretén aprofundir en l'enginyeria de programari realitzant el disseny de un component software de seguretat (IDTRAM - Identificació i detecció de tramvia) , que fent servir la infraestructura de la instal·lació tramviària existent (elements físics tant de terra com embarcats), detecti e identifiqui que sobre uns determinats carrils conductors hi ha un tramvia estacionat i garanteixi que únicament es donarà la ordre d'energitzar al sistema de carrega inferior de commutació, si el carrils conductors estan completament ocupats per el material mòbil.

El disseny del component software s'emmarca sota la norma UNE-EN 50128 de Març del 2012 que es la versió oficial de la norma europea EN 50128:2011 de obligat compliment per el desenvolupament de programari de seguretat relacionat amb el ferrocarril.

Per les connotacions sobre la seguretat de les persones que el component software IDTRAM presenta, té associat el nivell màxim de integritat de seguretat (SIL4) i cal que compleixi amb un conjunt de tècniques i mesures de integritat que la norma estableix per el seu desenvolupament. Al llarg de tot el disseny que s'ha dut a terme ha estat necessari identificar en tot moment el compliment de les tècniques i mesures adoptades en el desenvolupament del software.

Els principis aplicats en el desenvolupament del component son:

- Aplicació de mètodes de disseny descendents
- Modularitat
- Verificació de cada fase del cicle de vida
- Verificació dels components i de les llibreries que s'utilitzin
- Documentació i traçabilitat clares
- Documents auditables
- Validació
- Avaluació
- Gestió de la configuració i control de modificacions

1.2 Objectius del treball

L'objectiu del present treball es l'anàlisi i disseny del component software IDTRAM amb un nivell de integritat de la seguretat 4 (SIL 4) segons la norma UNE-EN 50128 2012 que ha de realitzar les següents funcions:

- Identificar la composició i el posicionament del material mòbil que accedeix i estaciona en cadascuna de les dues vies de una parada utilitzant els elements de camp existents que ja disposen de una interfície completament definida.
- Decidir quan es transfereix energia a cada carril conductor i ordenar al sistema de commutació l'activació dels elements pertinents. Aquest objectiu te connotacions relacionades amb la seguretat.
- Comprovar la integritat dels elements del sistema de commutació.
- Mantenir desactivats els elements del sistema de commutació quan es duguin a terme tasques de manteniment, quan ho sol·liciti el sistema de "telecomandament" de energia o quan es detectin problemes en el sistema de commutació en partícula en el interruptor automàtic de commutació.
- Bloqueig de la energització quan:
    - El Sistema de Informació i Monitorització (SIM) ho sol·liciti
    - El interruptor automàtic de commutació estigui fora de servei.
    - Supervisar, per cada via i per cada punt de parada, l'estat del sistema de commutació.

Els productes obtinguts s'indiquen en l'apartat 1.5 Breu sumari de productes obtinguts

1.3 Enfocament i mètode seguit

El compliment de la Norma UNE-EN 50128 per el desenvolupament de software de seguretat, obliga a utilitzar determinades tècniques i mesures, segons el nivell de seguretat que el component software tingui assignat, així com a establir un conjunt de plans que garanteixen el desenvolupament del software del sistema.

Per satisfer el nivell de integritat associat al component IDTRAM es faran servir les següents tècniques i mesures:

- Aproximació Modular
- Mòduls de mida limitada
- Encapsulació
- Un punt de entrada / un punt de sortida
- Interfícies completament definides

Mètodes semiformals

- Metodologia estructurades
- Programes analitzables
- Estàndards de disseny i codificació
- Registro i anàlisis de dades

La metodologia utilitzada serà orientada a objectes fent servir el model anomenat UML amb la utilització de les seves notacions i conceptes. Per l'anàlisi de requisits es faran servir diagrames de casos d'ús i diagrames de activitats que permetran obtenir requisits funcionals formals.

Per el disseny dels components es faran servir diagrames de components seguint la agrupació que s'indica a continuació:

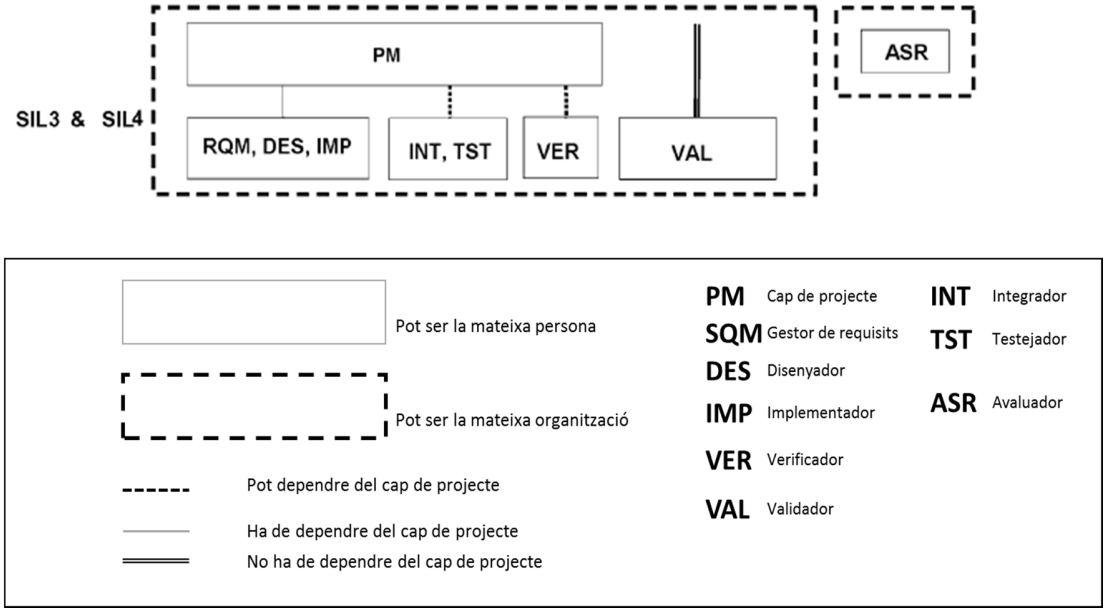
- Computer Software Configuration Item (CSCI) : Component software sotmès a control de la configuració
- Computer Software Component (CSC) : Un CSCI es descompon en un o mes CSC's
- Computer Software Unit (CSU) : Un element específic dins de un CSC. Un CSC pot tenir un o mes d' un CSC.

Per representar el intercanvi de missatges entre els diferents components, es faran servir els diagrames de seqüències

Per mostrar la transició entre els estats lògics es faran servir diagrames de estats.

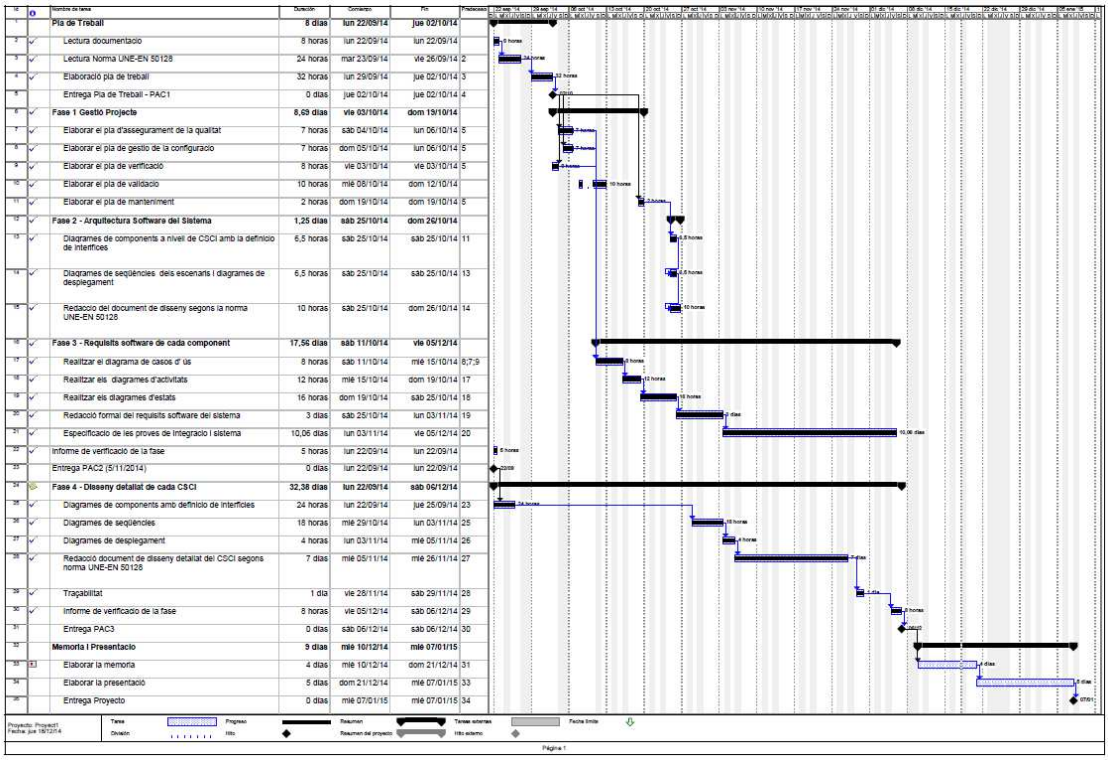
1.4 Planificació del treball

La norma obliga a disposar de una estructura organitzativa de forma que hi hagi independència entre diferents rols. Per el present projecte s'ha considerat aquest fet encara que tot el treball hagi estat realitzat per una persona. A continuació es mostra com hauria de ser la estructura de rols per el desenvolupament de un component software amb un nivell de integritat en la seguretat SIL4



Il·lustració 1 Estructura Organitzativa SIL4

A continuació es mostra el diagrama de Gantt que correspon a la planificació del projecte. En l'apartat 1.5 Breu sumari de productes obtinguts s'indica el codi que correspon al document de planificació



		Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**Pla de Treball**	**8 dias**	**lun 22/09/14**	**jue 02/10/14**	
2	✓	Lectura documentacio	8 horas	lun 22/09/14	lun 22/09/14	
3	✓	Lectura Norma UNE-EN 50128	24 horas	mar 23/09/14	vie 26/09/14	2
4	✓	Elaboració pla de treball	32 horas	lun 29/09/14	jue 02/10/14	3
5		Entrega Pla de Treball - PAC1	0 dias	jue 02/10/14	jue 02/10/14	4
6	✓	**Fase 1 Gestió Projecte**	**8,63 dias**	**vie 03/10/14**	**dom 19/10/14**	
7	✓	Elaborar el pla d'assegurament de la qualitat	7 horas	sab 04/10/14	lun 06/10/14	5
8	✓	Elaborar el pla de gestio de la configuracio	7 horas	dom 05/10/14	lun 06/10/14	5
9	✓	Elaborar el pla de verificació	8 horas	vie 03/10/14	vie 03/10/14	5
10	✓	Elaborar el pla de validacio	10 horas	mié 08/10/14	dom 12/10/14	
11	✓	Elaborar el pla de manteniment	2 horas	dom 19/10/14	dom 19/10/14	5
12	✓	**Fase 2 - Arquitectura Software del Sistema**	**1,25 dias**	**sab 25/10/14**	**dom 26/10/14**	
13	✓	Diagrames de components a nivel de CSCI amb la definicio de interfices	6,5 horas	sab 25/10/14	sab 25/10/14	11
14	✓	Diagrames de seqüències dels escenaris i diagrames de desplegament	6,5 horas	sab 25/10/14	sab 25/10/14	13
15	✓	Redaccio del document de disseny segons la norma UNE-EN 50128	10 horas	sab 25/10/14	dom 26/10/14	14
16	✓	**Fase 3 - Requisits software de cada component**	**17,56 dias**	**sab 11/10/14**	**vie 05/12/14**	
17	✓	Realitzar el diagrama de casos d' ús	8 horas	sab 11/10/14	mié 15/10/14	8;7;9
18	✓	Realitzar els diagrames d'activitats	12 horas	mié 15/10/14	dom 19/10/14	17
19	✓	Realitzar els diagrames d'estats	16 horas	dom 19/10/14	sab 25/10/14	18
20	✓	Redacció formal del requisits software del sistema	3 dias	sab 25/10/14	lun 03/11/14	19
21	✓	Especificacio de les proves de integracio i sistema	10,06 dias	lun 03/11/14	vie 05/12/14	20
22	✓	Informe de verificació de la fase	5 horas	lun 22/09/14	lun 22/09/14	
23		Entrega PAC2 (5/11/2014)	0 dias	lun 22/09/14	lun 22/09/14	
24		**Fase 4 - Disseny detallat de cada CSCI**	**32,38 dias**	**lun 22/09/14**	**sab 06/12/14**	
25	✓	Diagrames de components amb definicio de interfcies	24 horas	lun 22/09/14	jue 25/09/14	23
26	✓	Diagrames de seqüències	18 horas	mié 29/10/14	lun 03/11/14	25
27	✓	Diagrames de desplegament	4 horas	lun 03/11/14	mié 05/11/14	26
28	✓	Redacció document de disseny detallat del CSCI segons norma UNE-EN 50128	7 dias	mié 05/11/14	mié 26/11/14	27
29	✓	Traçabilitat	1 dia	vie 28/11/14	sab 29/11/14	28
30	✓	Informe de verificacio de la fase	8 horas	vie 05/12/14	sab 06/12/14	29
31		Entrega PAC3	0 dias	sab 06/12/14	sab 06/12/14	30
32		**Memoria i Presentacio**	**9 dias**	**mié 10/12/14**	**mié 07/01/15**	
33	✓	Elaborar la memoria	4 dias	mié 10/12/14	dom 21/12/14	31
34		Elaborar la presentació	5 dias	dom 21/12/14	mié 07/01/15	33
35		Entrega Proyecto	0 dias	mié 07/01/15	mié 07/01/15	34

Il·lustració 2 Planificació del projecte

1.5 Breu sumari de productes obtinguts

Producte obtingut	Codi
Memòria	IDTRAM-M014-MEM
Presentació	IDTRAM-PR015-PP(diapositives)
	IDTRAM-PR015_VID (vídeo)
Pla de treball	IDTRAM-P001-WP

Producte obtingut	Codi
Planificació del TFC	TFC_PT_010_Planificacio
Pla d'assegurament de la qualitat	IDTRAM-P002-SQAP
Pla de gestió de la configuració	IDTRAM-P003-SCMP
Pla de verificació del software	IDTRAM-P006-SVEP
Pla de validació del software	IDTRAM-P005-SVAP
Pla de manteniment del software	IDTRAM-P004-SMP
Especificació de la arquitectura Software del sistema	IDTRAM-A011-SSA
Registre de verificació de la arquitectura software del sistema	IDTRAM-VER012-SSA
Especificació de Requisits del component SIL4 IDTRAM	IDTRAM-R007-SR
Matriu de traçabilitat de requisits software del IDTRAM contra casos de prova	IDTRAM-PR008-MT
Especificació de les proves de integració i sistema	IDTRAM-PR008-SIT
	IDTRAM-PR008-ANNEX

Producte obtingut	Codi
Registre de verificació dels requisits software	IDTRAM-VER013-SR
Especificació de la arquitectura i disseny detallat del component IDTRAM	IDTRAM-D009-DS
Registre de verificació de la arquitectura i disseny del component IDTRAM	IDTRAM-VER014-SR
Matriu de traçabilitat de requisits software del IDTRAM contra els components del IDTRAM	IDTRAM-D009-MT

Taula 1 Relació de productes obtinguts

1.6 Breu descripció d'altres capítols

En el següent apartat es presenta el treball dut a terme. A continuació es descriu breument la seva estructura:

- Anàlisis de riscos : en aquest apartat es fa una breu descripció i anàlisi dels riscos
- Gestió del projecte : en aquet apartat s'identifiquen els plans del projecte i es descriu breument el seu contingut
- Arquitectura software del sistema: en aquest apartat es presenten els components CSCI del sistema indicant les seves responsabilitats i les seves interfícies.
- Requisits del component IDTRAM : en aquest apartat s'identifiquen i escriuen tots els requisits que el component IDTRAM ha de complir.
- Especificació de la arquitectura i disseny del component IDTRAM : en aquest apartat es mostra la descomposició del CSCI IDTRAM en diferents components

- Registres de verificació : en aquest apartat s'indiquen els registres de verificació realitzats i el seu resultat

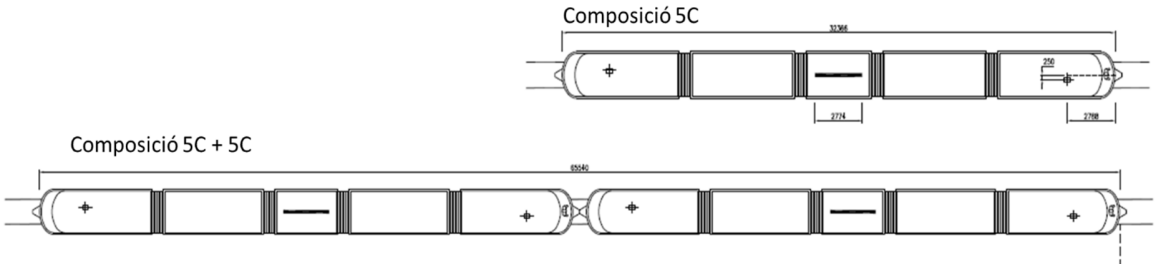
2 Projecte

2.1 Descripció

El sistema que ens ocupa es un subsistema dins del sistema de captació d'energia (d'ara en endavant CIE) que pren la decisió d'aplicar energia únicament en aquelles zones cobertes per una unitat mòbil.

El sistema de captació d'energia CIE té com a funció principal proporcionar energia elèctrica als tramvies dotats amb acumuladors de càrrega ràpida (ACR), quan circulen per les zones sense catenària. Quan el tramvia s'atura en alguna de les zones de càrrega es produeix el contacte elèctric mitjançant un grup de patins desplegables, situats en la part inferior del tramvia, i un conjunt de carrils conductors situats entre els carrils de rodament.

El CIE disposa en cadascuna de les dues vies de cada parada de quatre carrils conductors per poder donar servei de carrega inferior; els carrils conductors s'agrupen en parelles i estan associats a un punt de parada. El sistema únicament considera les unitats de tramvia amb composició simple 5C i amb composició doble 5C+5C



Il·lustració 3 Composició del material mòbil

Per les unitats de tramvia simples (composició 5C de la Il·lustració 3 Composició del material mòbil) es considera que normalment faran servir el mateix conjunt de dos carrils conductors per realitzar la carrega, aquesta posició es la denominada punt de parada

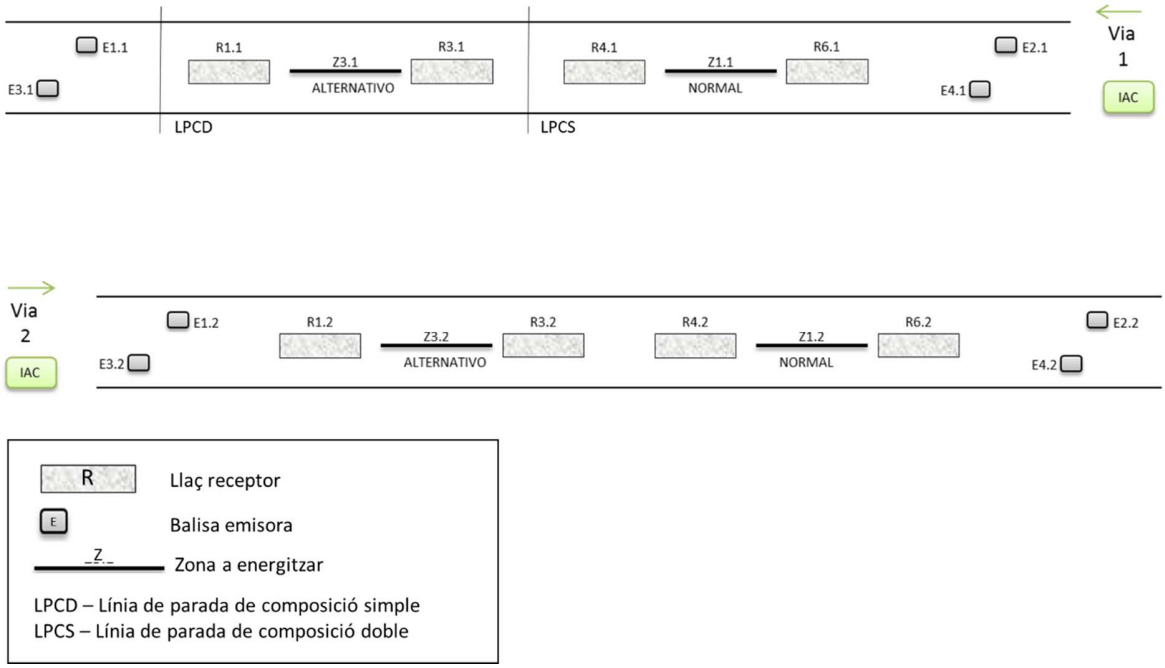
normal. En cas de incidència o averia es podrà fer la carrega mitjançat un altre parella de carrils denominada punt de parada alternativa.

La funció de IDTRAM es prendre la decisió d'aplicar energia únicament a aquells carrils conductors que corresponguin segons la posició i composició del material mòbil estacionat.

IDTRAM ha de garantir que únicament es doni la ordre de energia al CIE d'aquells carrils conductors quan el tramvia estigui completament detingut i correctament posicionat sobre la zona de carrega. Per tal de dur a terme aquesta funció s'utilitzarà l'equipament de via existent i equipament embarcat existent.

Per dur a terme les seves funcions IDTRAM fa us de la infraestructura existent formada per equipament instal·lat a via i per equipament embarcat en les unitats mòbils.

- L'equipament de via esta format per dispositius de comunicació i/o detecció instal·lats a via que tenen les següents funcions:
- Proporcionar a IDTRAM una interfície per identificar la composició dels tramvies que accedeixen a cadascuna de les dues vies de la parada
- Proporcionar a IDTRAM una interfície per determinar el posicionament dels tramvies a carregar.
- Establir un enllaç de comunicació entre el IDTRAM i cadascun dels tramvies a carregar.



Il·lustració 4 Infraestructura de via

L'equipament embarcat està ubicat en cadascuna de les cabines del tramvia. Las seves responsabilitats son:

- Enviar, a través del equipament de via, la informació necessària per tal que IDTRAM identifiqui el tipus de composició i el posicionament del tramvia.
- Rebre, a través del equipament de via, les informacions necessàries per assistir al conductor en la parada, per automatitzar la operació de baixada de patins i per informar al acumulador de carga ràpida (ACR) de les transicions entre les zones amb catenària i les zones sense catenària
- Transferir al automatisme intern del tramvia, les informacions del punt anterior.

Le interfícies que actuen amb el sistema per tal de rebre la informació dels elements de via consisteixen en entrades i sortides de seguretat i entrades i sortides auxiliars. Per comunicar-nos amb les entrades/sortides de seguretat es fa servir un component software ja existent anomenat COMSEG (Comunicador de seguretat) i per les entrades / sortides auxiliars i la comunicació amb les balises receptores i emissores, es fa servir un component software anomenat COBAL (Comunicació Balises)

2.2 Anàlisi de riscos

Tal i com s'esmenta en capítols anteriors, IDTRAM donarà ordre d'energitzar únicament quan la zona de carrega estigui completament coberta per una unitat mòbil, sempre i quan la integritat del sistema CIE es trobi garantida.

El principal risc resideix en el fet de donar ordre d'energitzar quan la zona de carrega no estigui completament coberta per una unitat mòbil o quan la integritat del CIE no es trobi garantida. A continuació s'analitzen les possibles situacions que poden desencadenar aquest risc i es fa un anàlisis de les seves conseqüències segons la classificació que s'indica en la Taula 2 Nivell de risc

Freqüència	**Nivell de risc**			
Freqüent	No desitjable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	No desitjable	Intolerable	Intolerable
Ocasional	Tolerable	No desitjable	No desitjable	Intolerable
Remot	Insignificant	Tolerable	No desitjable	No desitjable
Improbable	Insignificant	Insignificant	Tolerable	Tolerable
Increïble	Insignificant	Insignificant	Insignificant	Insignificant
	Insignificant	**Mínim**	**Crític**	**Catastròfic**
	Severitat			

Taula 2 Nivell de risc

Risc	Conseqüència	Seguretat		
		Freqüència	Severitat	Risc
Detecció de tramvia quan estant posicionat en la zona de captació, està mal posicionat. El tramvia no cobreix totalment el carril conductor	Ordre d'energització quan no hi ha tramvia posicionat i possible electrocució	Probable	Catastròfica	Intolerable
Detecció de tramvia parat quan esta en moviment	Ordre d'energització quan no hi ha tramvia i possible electrocució	Probable	Catastròfica	Intolerable
No es detecta que el tramvia ha abandonat la zona de captació	Ordre d'energització quan no hi ha tramvia i possible electrocució	Probable	Catastròfica	Intolerable
No es detecta el tramvia quan entra en la zona de captació	No es dona la ordre d'energitzar, possibles pèrdues materials	-	-	-
No es detecta correctament la composició del tramvia.	Ordre d'energització quan no hi ha tramvia i possible electrocució	Probable	Catastròfica	Intolerable
Recepció de informació de una determinada balisa i el sistema interpreta que es un altre	Ordre d'energització quan no hi ha tramvia i possible electrocució	Remot	Catastròfica	No desitjable
Error en la identificació del cap o de la cua del tramvia	Ordre d'energització quan no hi ha tramvia i possible electrocució	Probable	Catastròfica	Intolerable

Taula 3 Anàlisi de riscos

2.3 Gestió del projecte

La gestió del projecte compren el pla de treball i la seva planificació així com tots els plans que la norma indica per tal de garantir la qualitat del software en desenvolupament. Tots els plans han de ser fets al inici del projecte. Els documents relatius a la documentació i el seu

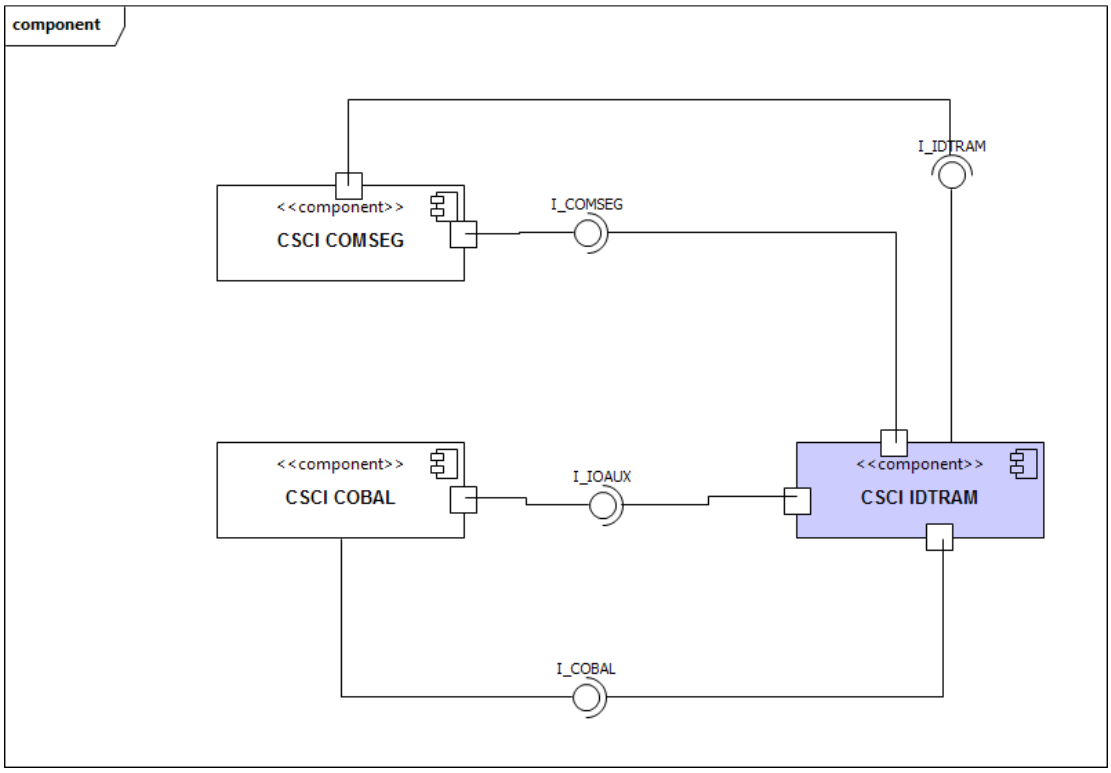
codi s'indiquen en l'apartat 1.5 Breu sumari de productes obtinguts. A continuació es fa una breu descripció dels plans existents.

- Pla d'assegurament de la qualitat que ha de complir amb la normativa ISO 9000 i ha de ser redactat per el verificador i cal que contingui informació relativa a :
    - El cicle de vida
    - Com es controla la documentació
    - Seguiment de la traçabilitat o de les desviacions
    - Com es notifiquen els problemes i quines son les accions correctives
    - Quines son les normes de codificació i quines son les mètriques aplicables
    - Quines son les eines, tècniques i metodologies utilitzades
    - Quina formació cal per l'equip de desenvolupament
- Pla de Gestió de la configuració que estableix com mantenir la integritat dels productes software al llarg de la seva vida. En el pla cal indicar:
    - Com es versionen els productes software
    - Quins son els components sotmesos a control de la configuració
    - Com es crearan les línies base
    - Com s'organitzarà el repositori
    - Quin es el procediment per la gestió del canvi
- Pla de manteniment on s'indica quines son les tasques a fer quan el software entri en la etapa de manteniment.
- Pla de verificació del software que te com a objectiu examinar i arribar a la conclusió basada en proves de que els elements de sortida de una fase del cicle de vida compleixen amb els plans relatius a la seva complexió , correcció i coherència
- Pla de Validació del software. La redacció d'aquest pla es responsabilitat del validador i ha de indicar quina es la estratègia de validació escollida segons el nivell de integritat del software.

2.4 Especificació de la arquitectura del sistema

L'objecte del projecte es l'estudi de com a de ser el component IDTRAM que forma part de un sistema software mes complex i que te assignada la funció de seguretat de detectar e identificar la unitat mòbil garantint que els carrils conductors on es donarà la ordre de energia estan completament coberts per el tramvia.

La especificació de la arquitectura software forma part del present treball per tal de clarificar el comportament general del sistema i mostra els CSCI del sistema indicant les seves responsabilitats i nivell de integritat de seguretat que tenen.



Il·lustració 5 Diagrama de components de la arquitectura software del sistema

La arquitectura software del sistema ha de donar com a mínim la següent informació:

- CSCI's que componen el sistema
- Responsabilitats de cada CSCI

- Interfícies que aporten
- Interfícies que fan servir
- Signatura de les operacions que formen part de les interfícies
- Comportament del sistema mitjançant escenaris que representen l'intercanvi de missatges entre components per dur a terme la funcionalitat associada
- Desplegament dels components

Una informació mes completa de la arquitectura del sistema es pot trobar en el document de arquitectura software del sistema ([2] IDTRAM-A011-SSA - Enginyeria de programari, 2014)

2.5 Especificació de requisits del component IDTRAM

En aquest capítol ja s'entra de ple en el disseny del component objecte del projecte amb la definició dels seus requisits ([4] IDTRAM-R007-SR Enginyeria de programari, 2014). La estructura i contingut del document de especificació de requisits es la següent:

- Identificació de la versió de requisits
- Descripció general del sistema: es fa una descripció breu del IDTRAM indicant les seves funcions. En aquest apartat es clarifica quines de les funcions son objecte del component i quines estan fora del seu abast.
- Consideracions de Safety: en aquest apartat es justifica el compliments de tots els punts de la norma relatius a la obtenció de requisits.
- Requisits del component: en aquest apartat s'identifiquen els requisits agrupats en subapartats. Cada subapartat correspon a un tipus de requisit i conté una taula on per cada requisit s'inclou un identificador, la seva descripció i la seva relació amb la seguretat. Els requisits s'agrupen en:
    - Requisits de interfície: son els relacionats amb les interfícies del sistema
    - Requisits de Safety : son tots aquells que tenen una especial relació amb la integritat del sistema.
    - Requisits de modus rellevants : descriuen les característiques especials dels modus de funcionament del sistema.

  - Requisits de seguretat informàtica: en aquest apartat s'indiquen els requisit de protecció de dades en el seu emmagatzemant i distribució
  - Requisits d' operació : els requisits d'operació s'obtenen a partir dels casos de ús i dels diagrames d'activitats. En l'apartat 6 del document es presenten els casos de us amb la seva descripció i els diagrames d'activitats de cada cas d'ús.
  - Requisits no funcionals : expressen capacitats i limitacions que cal tenir en compte.
- Taules de error : identifiquen i codifiquen els possibles errors detectats
- Traçabilitat de requisits del sistema que eren objecte del component que s'està dissenyant
- Glossari de termes
- Bibliografia

2.6 Especificació de proves de integració i sistema

La finalitat de la validació del software es demostrar que els processos i les seves sortides compleixen amb el nivell de integritat de seguretat assignat, que compleix amb els requisits software i que compleix amb les funcionalitats previstes. La validació del software ha de ser un procés independent de la resta i cal que el validador sigui una persona del departament de RAMS (*Reliability*, *Availability, Maintainability and Safety*).

La especificació de proves de integració i sistema compren tant les proves de dels requisits software del component com les proves de integració. Es a dir els casos de prova han de cobrir tots els requisits del IDTRAM i han de demostrar que la integració de les interfícies es comporta correctament.

Els casos de prova dels requisits han d'estar identificats amb un codi i es dissenyaran des de el punt de vista de caixa negra i lògica negativa. Cal incloure casos de prova que explotin condicions anòmales de funcionament, comprovin valors límits, exercitar els algoritmes del software fins arribar a situacions límits.

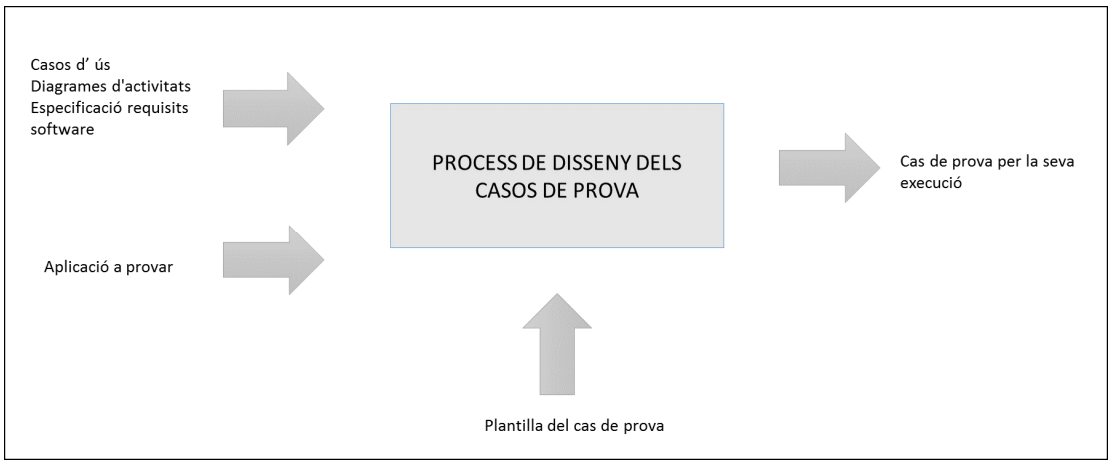
La especificació de proves de integració i sistema han de descriure l'entorn de proves amb la maqueta de proves i les explicacions necessàries per el seu muntatge. També ha de fer

esment de totes les eines de simulació necessàries per reproduir el comportament del tramvia i per reproduir l'entorn de la via.

En el IDTRAM es disposa per la realització de les proves de una maqueta física que reprodueix el comportament del COMSEG i una maqueta software que contempla el moviment del tramvia i les balises emissores i receptores que permeten el intercanvi de informació entre el tramvia i el IDTRAM

El procés que es segueix per el disseny dels casos de prova es el següent:

- Identificació de tots els escenaris presents en cada cas d' ús
- Identificació dels escenaris redundants procedint a la seva eliminació
- Identificació de les condicions d' execució de cada escenari
- Omplir la plantilla corresponent a cada cas de prova.



Il·lustració 6 Entrades i sortides del procés pel disseny dels casos de prova

Els casos de prova resultat han de ser optimitzats per obtenir una cobertura adequada de les proves amb el mínim nombre de casos de prova possibles i complint les següents característiques:

- El seu disseny ha de ser el mes senzill possible
- Han d'exercitar una característica del sistema que es vol provar

- Cal expressar les condicions necessàries per iniciar el cas de prova
- Tenir cura de minimitzar el numero de passos
- Tenir cura que cada cas de prova provi una sola característica
- Els casos de prova han de ser dissenyats de forma que es puguin tornar a repetir
- Cal indicar les precondicions així com els passos de la prova.

En el document ([3] IDTRAM-PR008-SIT - Departament RAMS, 2014) es troba la especificació de les proves de integració i sistema i en el document ([8] IDTRAM-PR008_ANNEX - Departament RAMS, 2014) es troben la bateria de casos de prova

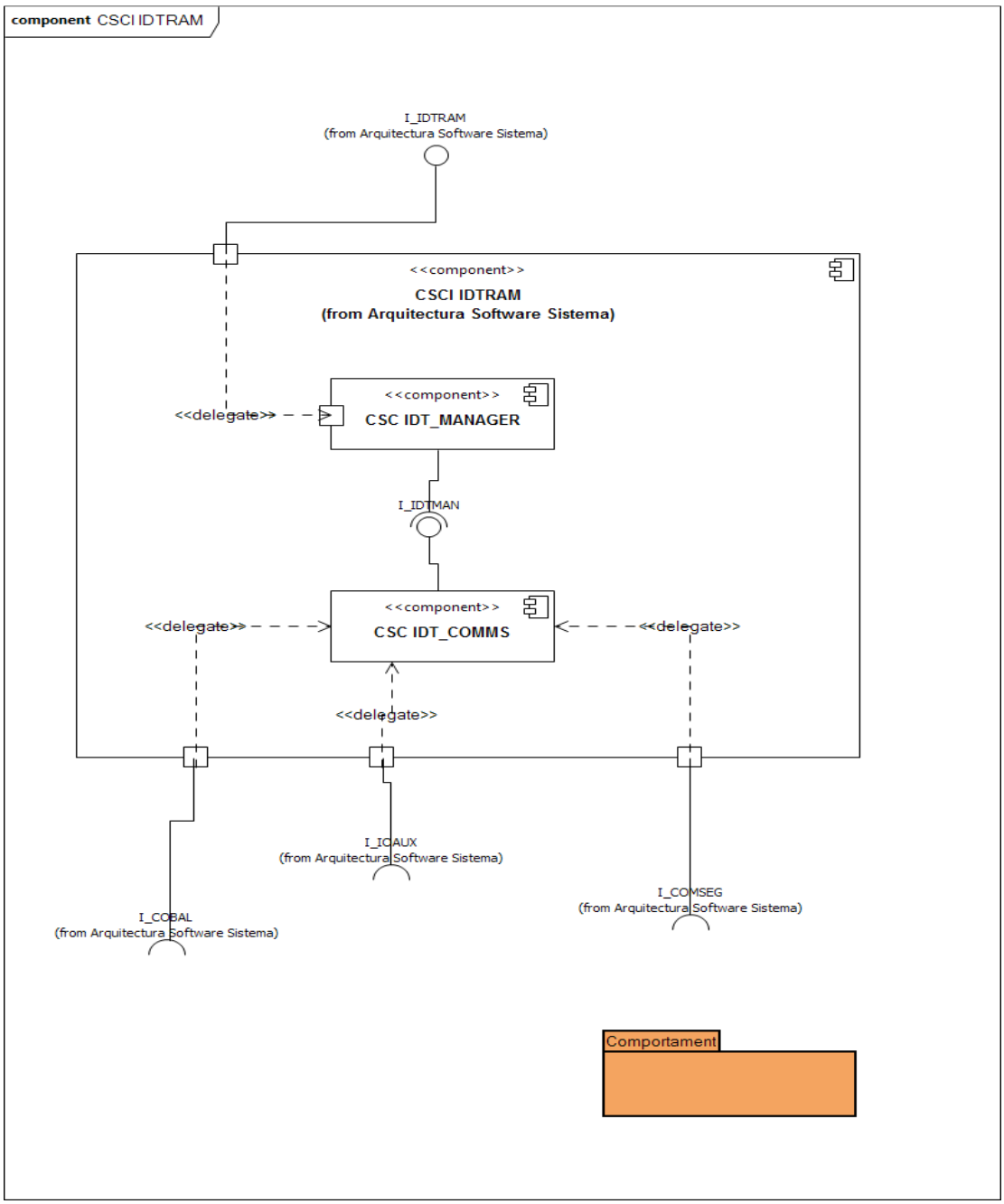
2.7 Especificació de la arquitectura i disseny detallat del component IDTRAM

Aquest document es divideix en dues parts clarament diferenciades: Una primera part on es descriu el component CSCI, s'indica la seva estructura i descomposició en CSC's, les seves responsabilitats, les interfícies aportades i utilitzades, el seu comportament i el seu desplegament i una segona part on s'entra en el disseny detallat de cada CSC indicant les seves responsabilitats, les CSU's que el composen, les interfícies aportades, el seu comportament i el seu desplegament.

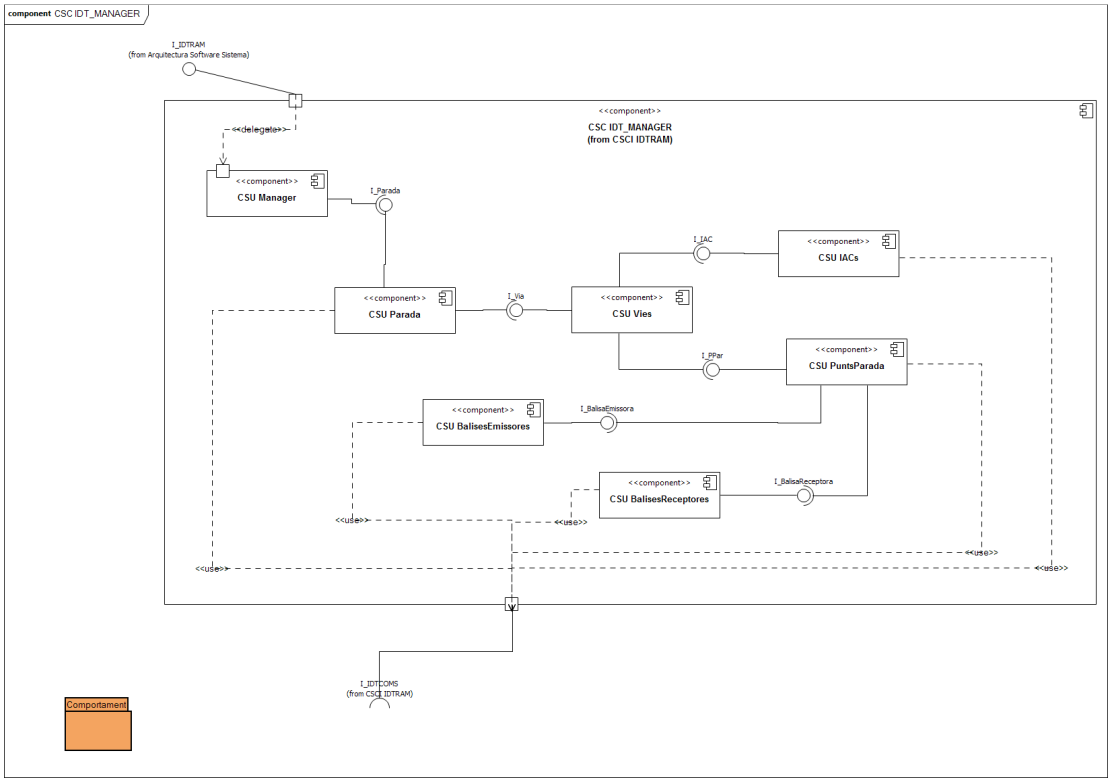
El document de disseny ha contenir els següents punts:

- Identificació de la versió del component
- Consideracions de Safety: en aquest apartat es justifica el compliments de tots els punts de la norma relatius a la obtenció de requisits.
- Decisions de disseny : en aquest apartat es dona una idea clara de la arquitectura del sistema en relació a la utilització de patrons existents, la selecció de tècniques escollides per complimentar el nivell de integritat de la seguretat associat al component. Algunes de les decisions de disseny venen heretades de la arquitectura software del sistema
    - Programació defensiva
    - Encapsulació
    - Patrons de disseny
    - Protecció contra errors

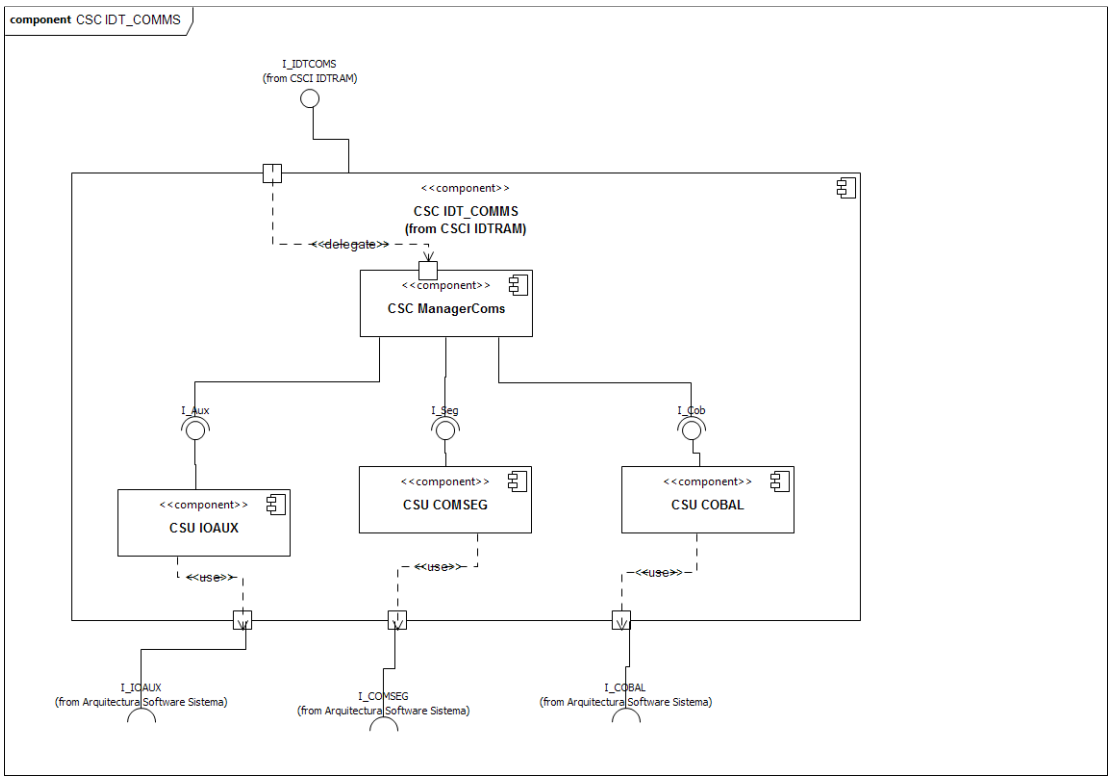
    - Redundància
    - Arquitectura amb doble processador
- Estructura del CSCI (Il·lustració 7 Estructura del CSCI IDTRAM) on es presenten els CSC's necessaris per complir totes les seves responsabilitats i tots els seus requisits
- Interfícies del CSCI : On es detallen les interfícies tant internes com externes i les seves operacions
- Comportament del CSCI : On mitjançant diagrames de seqüencia es mostres els escenaris adients. Cal mostrar el comportament amb el camí normal (happy path) i el comportament en situacions anòmales
- Desplegament del CSCI : On es presenta el desplegament del component en relació a la estructura de carpetes per els seu desenvolupament i el desplegament dins del mico mitjançant un diagrama de desplegament.
- Disseny detallat on es detalla cada CSC indicant:
    - La seva estructura en CSU's
    - Per cada CSU cal indicar:
        - Descripció
        - Interfícies que implementa i les seves operacions amb la signatura corresponent
    - Els diagrames de seqüencia que mostren el intercanvi de missatges entre les CSU's per complir amb un escenari determinat
    - El desplegament tant a nivell de desenvolupament indicant la estructura de carpetes i noms a fer servir com de ubicació dins del microprocessador amb un diagrama de desplegament
- La matriu de traçabilitat de requisits software contra components software per tal de comprovar que tots els requisits i tots els components estan traçats



Il·lustració 7 Estructura del CSCI IDTRAM



Il·lustració 8 Diagrama de components del CSC IDT_MANAGER



Il·lustració 9 Diagrama de components del CSC IDT_COMMS

El document ([1] IDTRAM-D009-DS - Enginyers de desenvolupament, 2014) es pot trobar la arquitectura i disseny del component CSCI IDTRAM

2.8 Registres de verificació

Registres de verificació	Codi
Registre de verificació de la arquitectura software del sistema	IDTRAM-VER012-SSA
Registre de verificació dels requisits software	IDTRAM-VER013-SR

Registres de verificació	Codi
Registre de verificació de la arquitectura i disseny del component IDTRAM	IDTRAM-VER014-SR

Taula 4 Registres de verificació

Els registres de verificacions son realitza per el verificador i tenen com a finalitat comprovar que els productes obtinguts en la fase corresponent compleixen amb els punts establerts en el pla de verificació ([6] IDTRAM-P006-VER - Direccio del projecte, 2014)

Per cada fase es documenten les desviacions i s'avalua si es pot continuar a la següent fase o no. En cas de que es pugui continuar endavant, cal arreglar les desviacions en la propera revisió

3 Conclusions

Tal i com he indicat en el apartat 1.1 Context i justificació del treball el propòsit del treball era aprofundir en l'àrea de l'enginyeria de programari i en particular quan el disseny del software està lligat a una normativa molt estricta de seguretat.

Fent una valoració de la feina feta, val a dir que els coneixements aplicats han estat adquirits en diverses assignatures de la carrera però també coneixements adquirits en el treball diari. La realització del treball m'ha obligat a treballar mes acuradament la normativa aplicable i a veure com es podia encabir dins del modelatge per UML.

No he assolit tots els objectius que inicialment m'havia plantejat, però si que he aclarit conceptes que fins ara no estaven clars. Penso que el problema mes gran es el fet que entendre la normativa implica un esforç important difícil de realitzar en el temps que tenim per realitzar el treball final de carrera.

En quan al seguiment de la planificació crec que ha estat correcta, si be la segona PAC es va veure afectada per el fet que la especificació de proves de integració i sistema va resultar

mes laboriosa que el que jo esperava. D'altra banda en els document de disseny del component es troben a faltar diagrames de seqüencies que reflecteixen el comportament davant de situacions anòmales.

La metodologia seguida crec que es la correcta i s'adapta als punts que la normativa exigeix. En aquest punt han quedat encara difusos la representació de les comunicacions sèrie en el model UML. En un futur seria convenient millorar els coneixements de UML per tal de poder modelar mes acuradament.

4 Glossari

Glossari

Nom	Descripció
IDTRAM	Identificació i Detecció de Tramvies
IAC	Interruptor Automàtic de Commutació
CIE	Carrega Inferior i Energització
SIM	Sistema de Informació i Monitorització.
ICAT	Identificació de cabina en tramvia
COMSEG	Comunicador de seguretat
COBAL	Comunicació Balises
CSCI	Computes Software Configuration Item
CSC	Computer software component
CSU	Computer software unit

5 Bibliografia

[1] IDTRAM-D009-DS - Enginyers de desenvolupament. (2014). Arquitectura i disseny del component CSCI IDTRAM.

[2] IDTRAM-A011-SSA - Enginyeria de programari. (2014). IDTRAM-A011-SSA - Arquitectura Software del sistema.

[3] IDTRAM-PR008-SIT - Departament RAMS. (2014). IDTRAM-PR008-SIT Proves de integració i sistema del IDTRAM.

[4] IDTRAM-R007-SR Enginyeria de programari. (2014). IDTRAM-R007-SR - Especificacio de requisits software del CSCI IDTRAM.

[6] IDTRAM-P006-VER - Direccio del projecte. (2014). Pla de verificació del software.

[8] IDTRAM-PR008_ANNEX - Departament RAMS. (2014). RAMS, IDTRAM-PR008_ANNEX Annex de bateria de proves de validacio.

[9], C. (2011). Norma EN 50128, Marzo 2012 - Aplicaciones ferroviarias.