ISO 26262
Application Example
(Connected & Downloadable Infotainment Platform)

Rustam Rakhimov
(DMS Lab)

Contents

(Derived from kVA Training Practical Exercises)

- Introduction about the Project
- Safety Management and Safety Lifecycle
  - Using checklist
  - Managing traceability
- Hazard Analysis, Risk Assessment, and ASIL Determination
  - Item description and hazard analysis
  - ASIL Determination using ISO 26262
- Functional safety at the system level
  - FTA at system level
- Hardware and Software Solutions
- Little-bit about CMMI

Introduction About Project

- Connected & Downloadable Infotainment Software platform for the Vehicular IT Convergence Service
- Eco-system of the IT Convergence Software based on the C&D Infotainment Software Platform

Sub-Projects

Connected Vehicle Platform

- Vehicular Application Processor
- Open Hardware Platform and the Testbed
- In-Vehicle/Out-Vehicle Network Support
- Connectivity Service

C&D Infotainment System

- Convergence Gateway for the Telematics Service
- Automotive Killer Applications

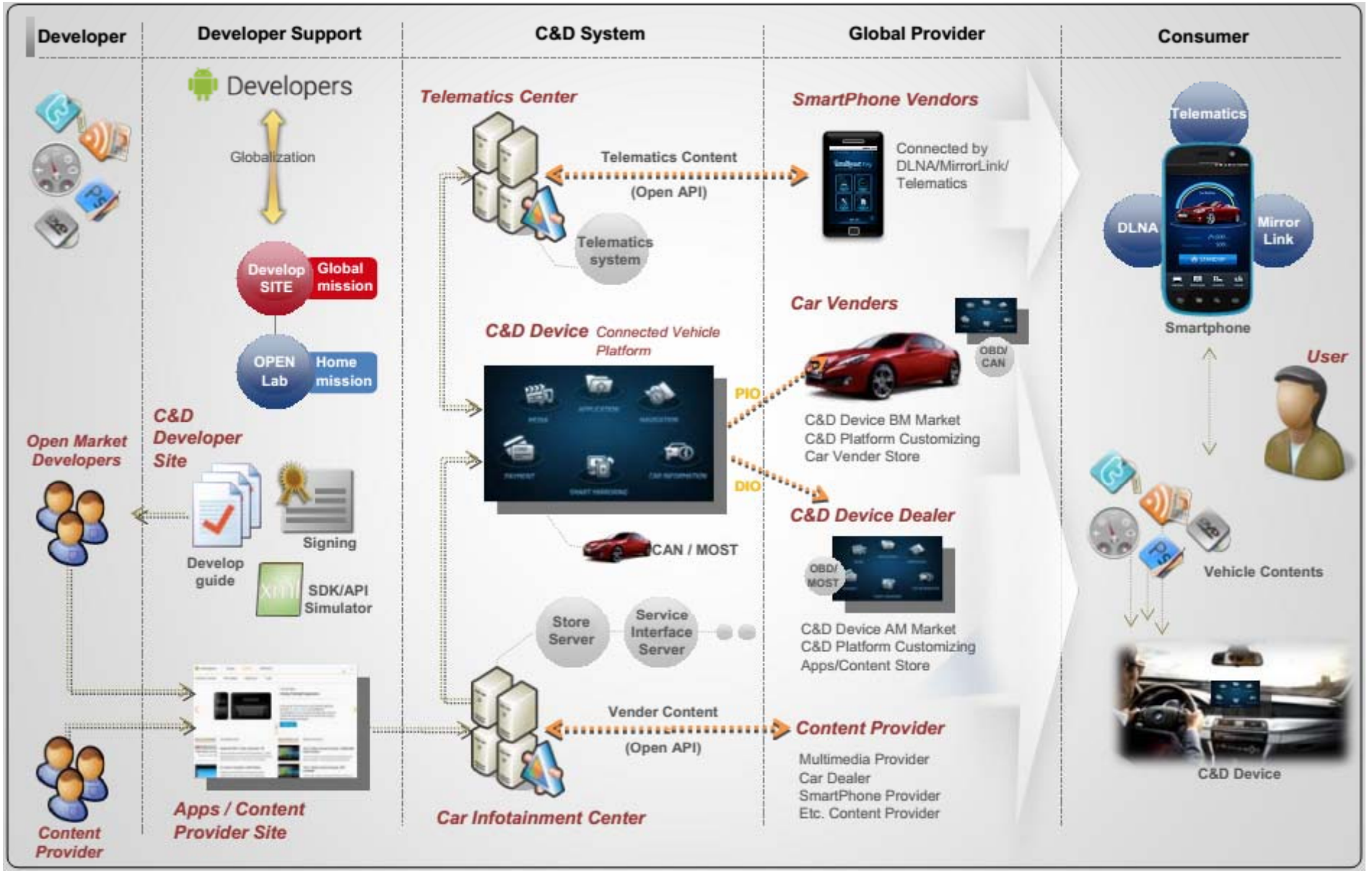
Downloadable Service Platform

- Open Automotive IT Convergence App. Platform
- Efficient Software Platform
- Standardized Automotive Open API
- Software Development Kit inc. the Vehicle Emulator
- Vehicle-specialized AppStore

Eco-system

- OpenLab Establishment
- Globalization
- Support of Certification

C&D Global Eco-System



Safety Management and Safety Lifecycle

- Using checklist
-Managing traceability

- **Checklists**
- Prerequisites
  - Organization-specific rules and processes for functional safety (in accordance with 5.5.1)
  - Evidence of competence (in accordance with 5.5.2)
  - Evidence of quality management (in accordance with 5.5.3)
- Optional (If available)
  - Project plan (from external source) - Fixed with UBIVELOX
  - Dependencies on other activities, including other safety activities

- **Traceability**
- A traceability is provided at following levels:
  - Management
  - Engineering
  - Development processes
- And not provided on following levels:
  - Verification
  - Validation
  - Functional Safety Audit
  - Functional Safety Assessment

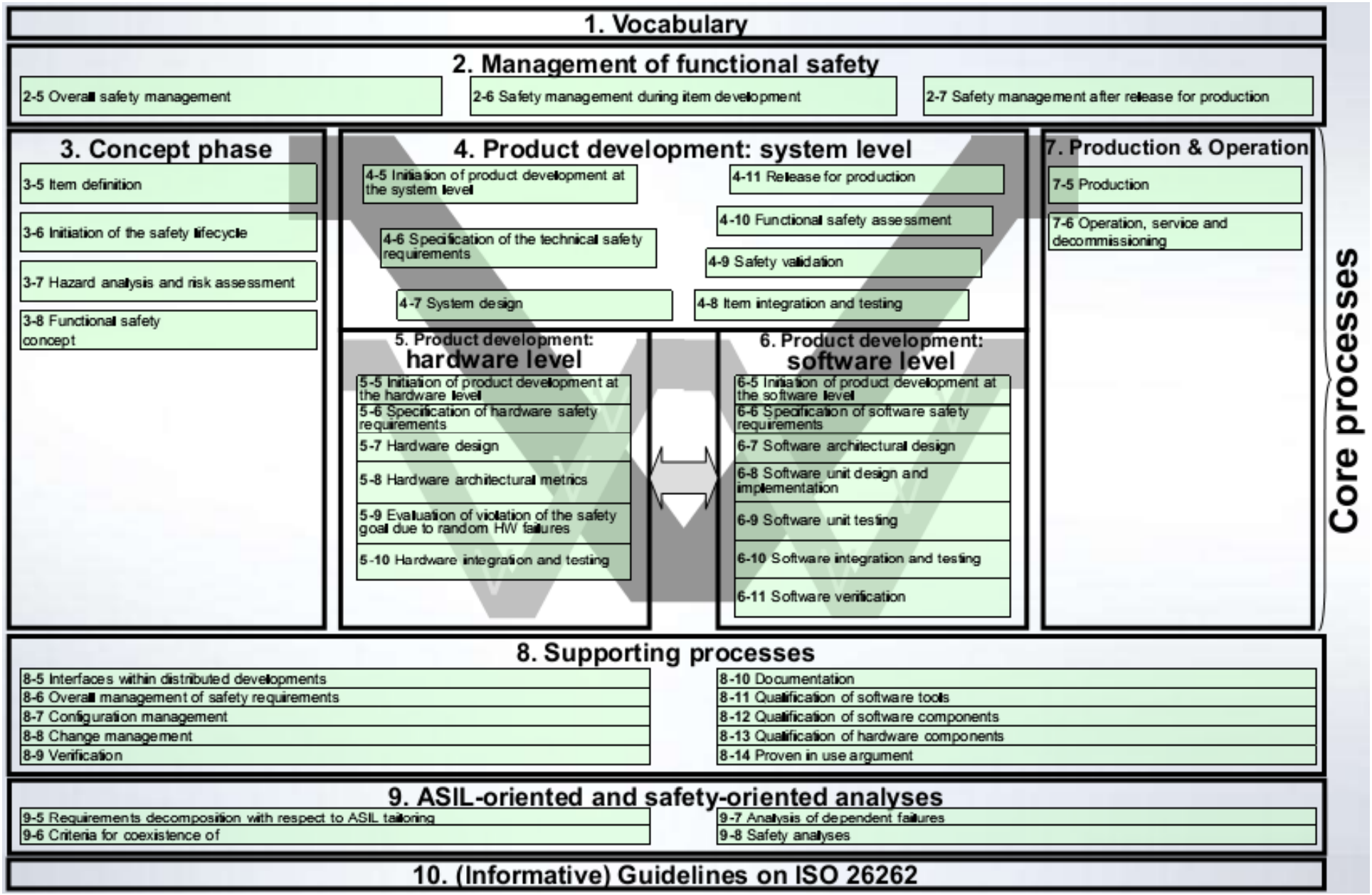
Item Definition: Specs Presented by KETI

ID	SPEC TYPE	SPEC NAME
SPEC01	SDS	MOST Automotive API SDS
SPEC02	SAS	MOST Automotive API SAS
SPEC03	SIS	MOST Automotive API SIS
SPEC04	SRS	MOST Automotive API SRS
SPEC05	SAS	MOST Low Level Driver SAS
SPEC06	SDS	MOST Low Level Driver SDS
SPEC07	SIS	MOST Low Level Driver SIS
SPEC08	SRS	MOST Low Level Driver SRS
SPEC09	SAS	MOST Media Player SAS
SPEC10	SDS	MOST Media Player SDS
SPEC11	SIS	MOST Media Player SIS
SPEC12	SRS	MOST Media Player SRS
SPEC13	SAS	MOST Media Server SAS
SPEC14	SDS	MOST Media Server SDS
SPEC15	SIS	MOST Media Server SIS
SPEC16	SRS	MOST Media Server SRS

Item Definition: Traceability Matrix Documents

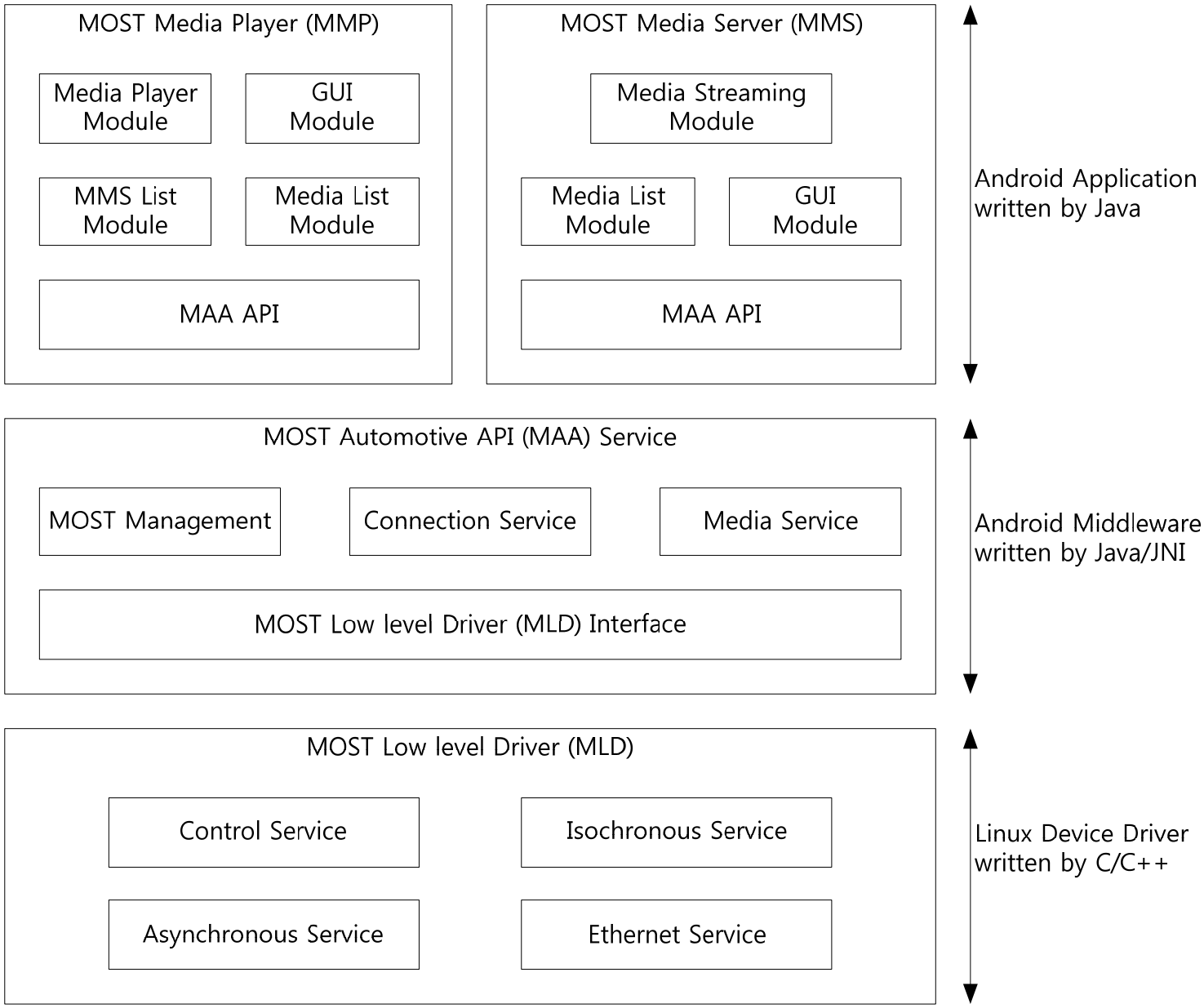
ID	Name
TM01	MOST Automotive API Traceability Matrix
TM02	MOST Low Level Driver Traceability Matrix
TM03	MOST Media Player Traceability Matrix
TM04	MOST Media Server Traceability Matrix
TC01	CND Test Case: MOST

General Structure of ISO 26262



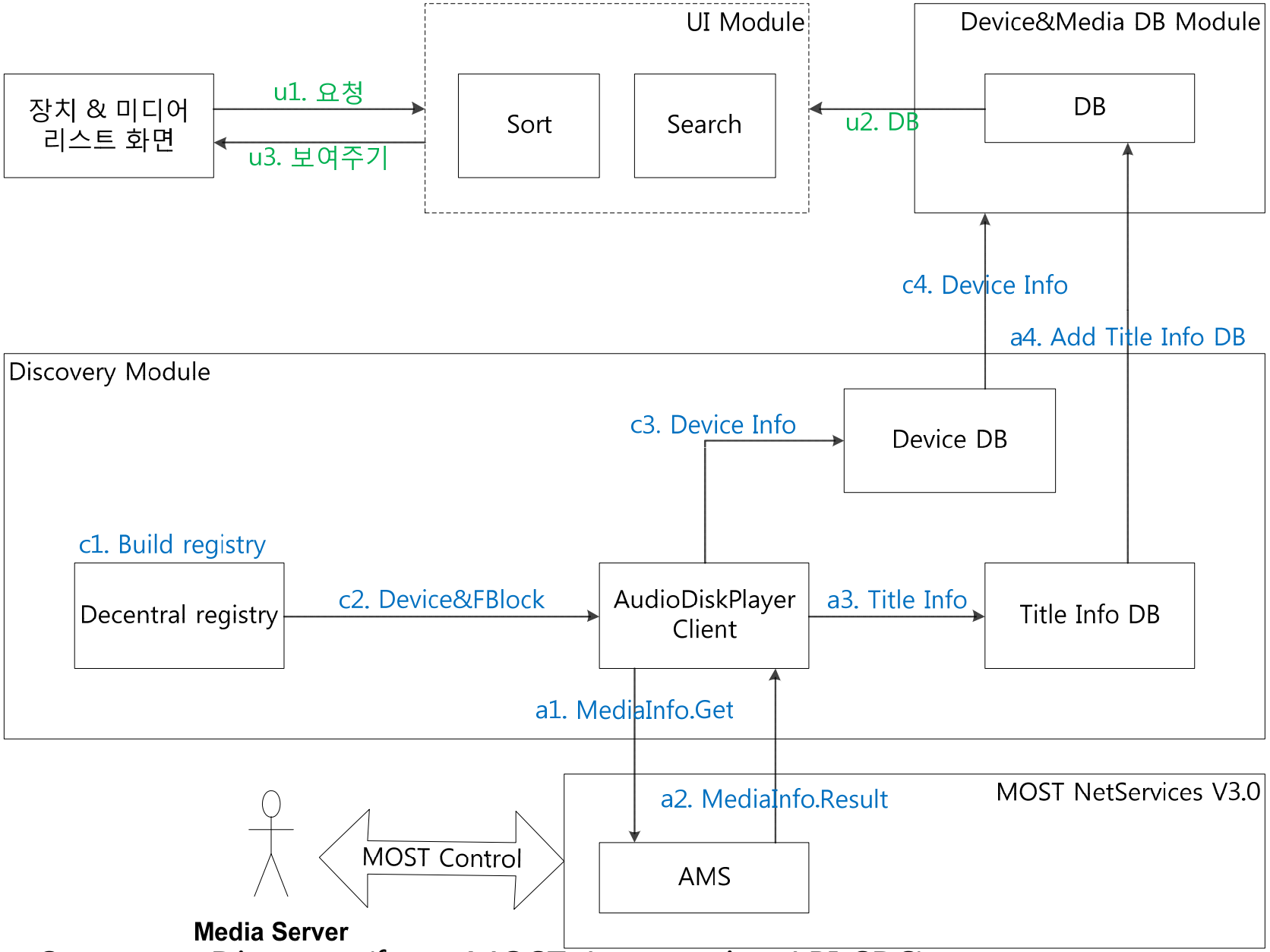
Walk through the given documents

System Level Analysis



- System Architecture (from MOST Automotive API SAS)

System Level Analysis



- Sequence Diagram (from MOST Automotive API SDS)

System Level Analysis

- **Generate MMS List [CC-UC01: Generate MMS List]**

c1) Build the MOST Decentral registry
c2) FBlock 내용 전달
c3, c4) 장치 정보 전달

- **Get MMS List [CC-UC10: Get MMS List]**

u1) 요청
u2) MMS 목록 전달
u3) MMS 목록 전달

- **Update MMS List [CC-UC02: Update MMS List]**

사용자의 갱신 요청이 있을 경우 Generate MMS List를 반복한다.

- **Get Media List [CC-UC11: Get Media List]**

a1) MediaInfo.Get 송신
a2) MediaInfo.Result 수신
a3) Media의 타이틀 정보 추출 후 DB 구성
a4) DB에 추가

- **Generate Media List [CC-UC04: Generate Media List]**

a1) 미디어 리스트 구성 요청
a2) 미디어 파일 검색
a3) 미디어 목록 구성 후 DB에 추가

- **Set Media List [CC-UC12: Set Media List]**

c) 미디어 리스트 핸들 전달

- **Respond Media List [CC-UC11: Get Media List]**

b1) Receive the MediaInfo.Get
b2) Search the Information to send
b3) Respond the MediaInfo.Result

- **Request to Start Streaming [CC-UC08: Connect, CC-UC16: Open]**

a1) 사용자로부터 스트리밍 시작 Command 입력
a2) Open 명령 전달
a3) Allocate.Set 전송
a4) Allocate.Result 응답 수신
  - **Start/Control/Stop Streaming [CC-UC07: Control Streaming]**

a1) 사용자로부터 Control Command 입력
a2) Start/Control/Stop 제어 명령 전달
a3) 제어 메시지 전송
a4) 제어 메시지의 응답 수신

- **Receive Media[CC-UC06: Receive Media,CC-UC14: Read]**
- **Start Streaming[CC-UC08: Connect, CC-UC16: Open]**

a1) 스트리밍 시작 요청 수신
a2) Connection 수립 요청 (Open)
a3) Allocate 요청 메시지 전송

- **Transmit Streaming [CC-UC05: Transmit Media, CC-UC13: Write]**

a4) 스트리밍 시작

- **Stop Streaming [CC-UC09: Disconnect, CC-UC15: Stop Streaming, CC-UC17: Close]**

a1) 스트리밍 종료 요청 수신
a2) Connection 제거 요청 (Close)
a3) Deallocate 요청 메시지 전송
a4) 스트리밍 종료

- Sequence Diagram Descriptions (from MOST Automotive API SDS)

Software Interface

GetDeviceInfo
Purpose: 장치 정보를 요청한다.
INPUT: Device handle (NULL일 경우 자신의 장치 정보)
OUTPUT: DeviceInfo

SetDeviceInfo
Purpose: 장치 정보를 설정한다.
INPUT: DeviceInfo
OUTPUT: N/A

GetDeviceList
Purpose: 전체 장치 목록의 첫 번째 핸들을 얻는다.
INPUT: DeviceType (NULL이면 모든 종류의 장치)
OUTPUT: Device handle

NextDevice
Purpose: 입력된 장치 핸들의 다음 장치의 핸들을 얻는다.
INPUT: Device handle
OUTPUT: Device handle

PrevDevice
Purpose: 입력된 장치 핸들의 이전 장치의 핸들을 얻는다.
INPUT: Device handle
OUTPUT: Device handle

FindDevice
Purpose: 입력된 정보를 바탕으로 장치를 찾고 해당 핸들을 얻는다.
INPUT: 검색 정보
OUTPUT: Device handle

Use Case ID	SRS ID
CC-UC1	SRS-MMS-001 ~ 004
CC-UC2	SRS-MMS-001 ~ 003
CC-UC3	SRS-MMS-001 ~ 003
CC-UC10	SRS-MMS-001 ~ 004

- Discovery Device (from MOST Automotive API SIS)

Software Interface

AddMediaInfo
Purpose: 미디어 파일 정보를 추가한다.
INPUT: MediaInfo
OUTPUT: N/A

RemoveMediaInfo
Purpose: 미디어 파일 정보를 삭제한다.
INPUT: MediaInfo
OUTPUT: N/A

ClearAllMedia
Purpose: 모든 미디어 파일 정보를 삭제한다.
INPUT: N/A
OUTPUT: N/A

GetMediaInfoList
Purpose: 미디어 파일 목록의 첫 번째 미디어 파일의 정보를 얻는다.
INPUT: N/A
OUTPUT: MediaInfo handle

Use Case ID	SRS ID
CC-UC4	SRS-MMS-001 ~ 004
CC-UC11	SRS-MMS-001 ~ 004
CC-UC12	SRS-MMS-001 ~ 002

NextMediaInfo
Purpose: 다음 미디어 파일 정보를 얻는다.
INPUT: MediaInfo handle
OUTPUT: MediaInfo handle

PrevMediaInfo
Purpose: 이전 미디어 파일 정보를 얻는다.
INPUT: MediaInfo handle
OUTPUT: MediaInfo handle

FindMediaInfo
Purpose: 입력된 정보를 바탕으로 미디어 파일을 찾는다.
INPUT: 검색 정보
OUTPUT: MediaInfo handle

- Discovery Media (from MOST Automotive API SIS)

Software Interface

Use Case ID	SRS ID
CC-UC5	SRS-MMS-001 ~ 005
CC-UC6	SRS-MMS-001 ~ 004
CC-UC13	SRS-MMS-001 ~ 002
CC-UC14	SRS-MMS-001
CC-UC18	SRS-MMS-001 ~ 004

Write
Purpose: 스트리밍 데이터를 송신한다.
INPUT: 스트리밍 데이터, 길이
OUTPUT: N/A

Read
Purpose: 스트리밍 데이터를 수신한다.
INPUT: 길이
OUTPUT: 스트리밍 데이터

Connect
Purpose: 스트리밍을 요청한다.
INPUT: 대역폭 (Quadlet 개수)
OUTPUT: N/A

Disconnect
Purpose: 스트리밍을 종료한다.
INPUT: N/A
OUTPUT: N/A

GetStatistics
Purpose: 스트리밍 통계정보를 요청한다.
INPUT: N/A
OUTPUT: 통계 데이터

- Streaming (from MOST Automotive API SIS)

Software Interface

Play

Purpose: 미디어를 재생한다
INPUT: N/A
OUTPUT: N/A

Pause

Purpose: 재생을 일시 멈춘다.
INPUT: N/A
OUTPUT: N/A

Stop

Purpose: 재생을 중지한다.
INPUT: N/A
OUTPUT: N/A

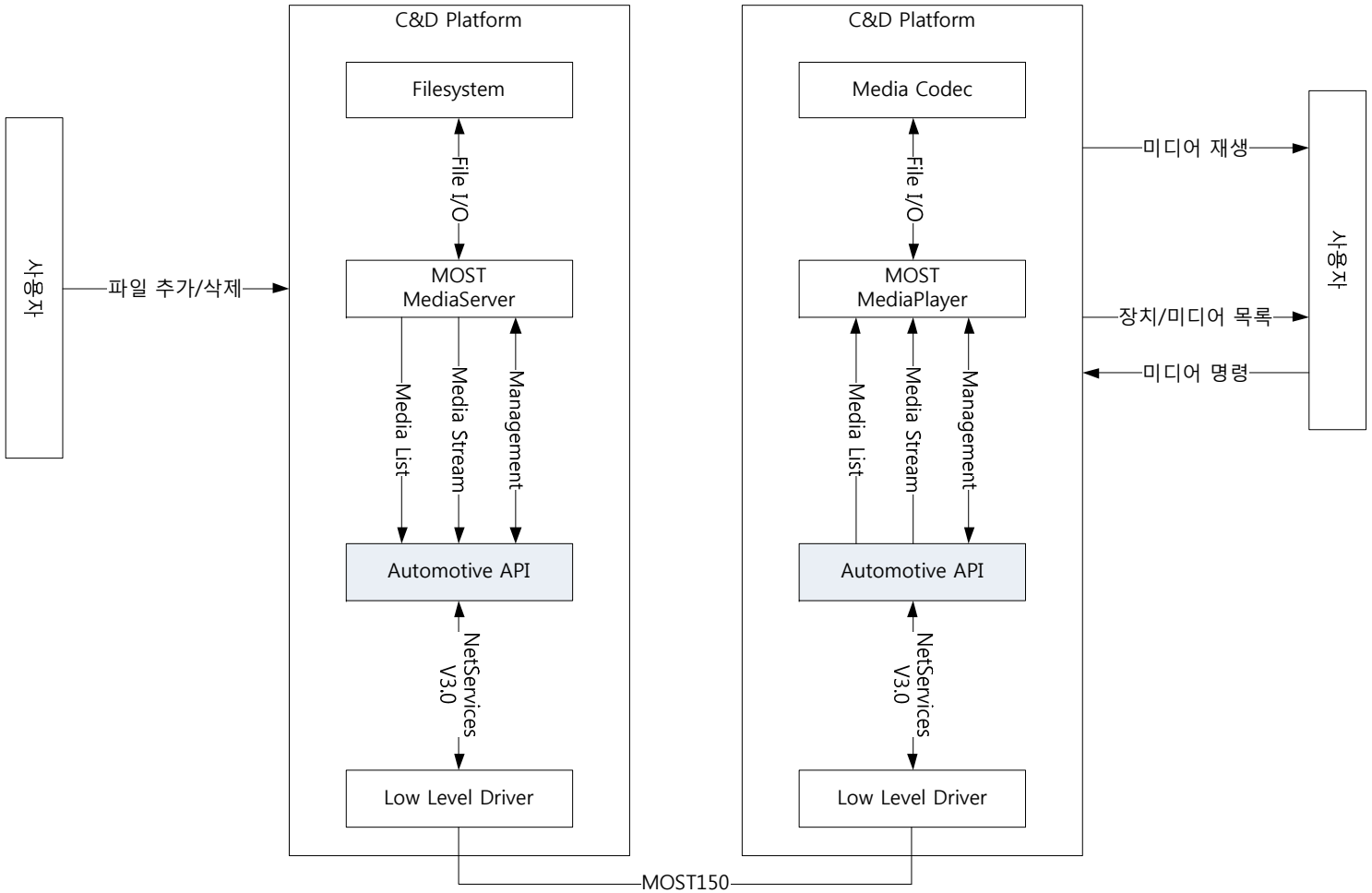
Volume

Purpose: 볼륨을 조절한다.
INPUT: 볼륨값
OUTPUT: 새로운 볼륨값

Use Case ID	SRS ID
CC-UC7	SRS-MMS-001
CC-UC8	SRS-MMS-001 ~ 002
CC-UC9	SRS-MMS-001
CC-UC15	SRS-MMS-001
CC-UC16	SRS-MMS-001
CC-UC17	SRS-MMS-001

- Media Player Control (from MOST Automotive API SIS)

Software Context



- C&D Platform Context Diagram (from MOST Automotive API SRS)

Software Major Function

서비스 상세 (Feature List)	설명
AudioDiskPlayer FBlock DB 구성	[MMP] Registry등록된 AudioDiskPlayer FBlock들과 통신으로 컨텐츠 정보를 수집해 데이터베이스를 만드는 기능을 제공한다.
Media Control Service	[MMP] MMP에서 요청한 재생 제어 메시지를 해당 장치에 전달하고 응답 결과를 보고하는 기능을 제공한다.
Recv MediaStreaming	[MMP] MMS에서 전송한 미디어 스트리밍 데이터를 Iso채널로 수신해 MMP에 전달하는 기능을 제공한다.
미디어 브라우징	[MMP] AudioDiskPlayer FBlock DB데이터를 MMP에게 제공한다.
미디어 목록으로 FBlock구성	[MMS] MMS가 만들어 놓은 미디어 목록을 AudioDiskPlayer FBlock의 Magazine과 ActiveDisk로 구성해 FBlock의 컨텐츠를 완성하는 기능을 제공한다.
Send MediaStreaming	[MMS] MMS에서 요청한 미디어 스트리밍 데이터를 Iso채널로 전송하는 기능을 제공한다.
세션 추가	MMP에서 재생 요청이 있을 경우, 요청한 미디어를 전송해 줄 MMS와 이를 수신할 MMP 사이에 Iso채널을 할당하는 기능을 제공한다.
세션 제거	MMP에서 미디어 서비스가 종료되거나 새롭게 요청한 미디어가 다른 장치에 위치할 경우 이전에 사용하던 세션의 연결을 해제하는 기능을 제공한다.
미디어 목록 서비스	MMP는 미디어 목록을 MMS에 요청하고 MMS는 MMP에게 미디어 목록을 제공하는 기능을 제공한다.

- C&D Platform Context Diagram (from MOST Automotive API SRS)

Software Classification

액터 도출

액터명	액터 설명	비고
MOST Media Server (MMS)	MMS 응용 프로그램	
MOST Media Player (MMP)	MMP 응용 프로그램	
Media API	MOST Low Level Driver 모듈	
Media Device API	미디어 파일이 저장되어 있는 파일 시스템	
Connection API		
MOST Device API		
Registry	NetworkMaster인 경우에는 Central Registry이고 NetworkSlave일 경우에는 Decentral Registry	

Device Manager

유스케이스 ID	유스케이스명	관련 액터	관련 SyRS
CC-UC1	Generate MMS List	Registry Media Device API	
CC-UC2	Update MMS List	Registry Media Device API	
CC-UC3	Gen MOST Device List		

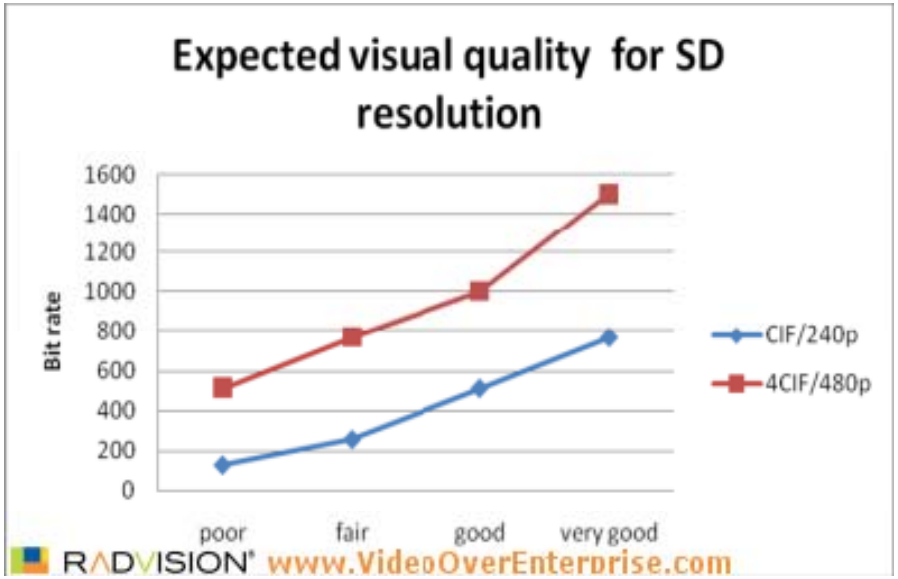
Media Manager

유스케이스 ID	유스케이스명	관련 액터	관련 SyRS
CC-UC4	Generate Media List	Media API Media Server	
CC-UC5	Transmit Media	Media API Media Server	
CC-UC6	Receive Media	Media API Media Server	
CC-UC7	Control Streaming	Media API Media Server Media Player	

- C&D Platform Context Diagram (from MOST Automotive API SRS)

Quality Attribute

- 영상 데이터의 크기는 480p 규격을 따른다.
- MOST Automotive API 에 의해 전달되는 영상 스트리밍 데이터는 SD급 비디오 데이터의 Fair 수준의 품질을 갖으며 아래 그림과 같은 대역폭 기준에 따라 480p 영상으로 1Mb/s 대역폭을 갖는다.
- MOST Applicatioin 과 MOST LLD 간의 컨텍스트 교환에 요구되는 지연 시간은 MOST NetServices가 포함된 LLD의 WatchDog 타이머 시간을 고려하여 결정되는데 MOST NetServices의 WatchDog 타이머의 최대값인 500ms 이내로 한다.



- C&D Platform Context Diagram (from MOST Automotive API SRS)

Most Automotive API Traceability Matrix

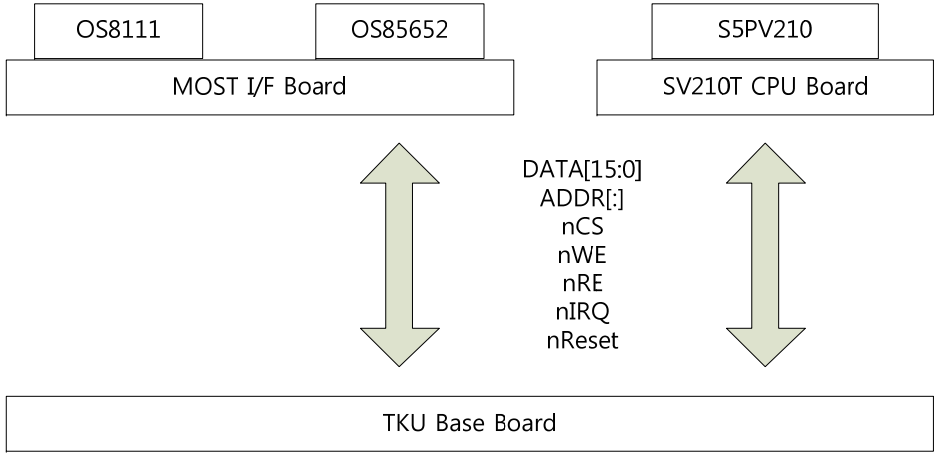
MAA SIS Traceability Matrix		Generate MMS List	Update MMS List	Gen MOST Device List	Generate Media List	Transmit Media	Receive Media	Control Streaming	Connect	Disconnect	Get MMS List	Get Media List	Set Media List	Write	Read	Stop Streaming	Open	Close	Statistics
Requrement Identifiers		CC-UC1	CC-UC2	CC-UC3	CC-UC4	CC-UC5	CC-UC6	CC-UC7	CC-UC8	CC-UC9	CC-UC10	CC-UC11	CC-UC12	CC-UC13	CC-UC14	CC-UC15	CC-UC16	CC-UC17	CC-UC18
Software Interface																			
1	DiscoveryDevice	x	x	x							x								
2	DiscoveryMedia				x							x	x						
3	Streaming					x	x							x	x				x
4	Media Player Control							x	x	x						x	x	x	

MOST Low Level SAS

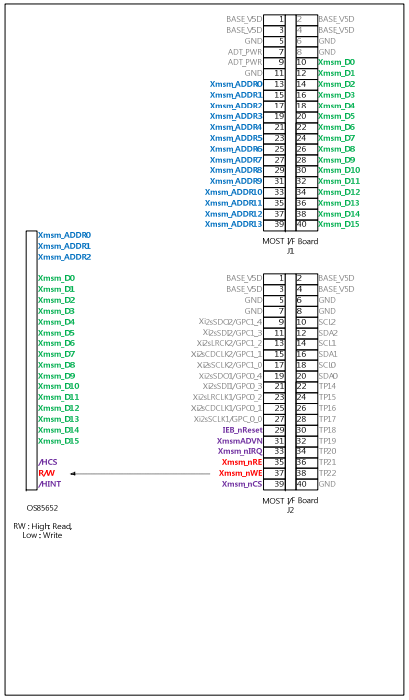
- C&D Platform 하드웨어에서 사용하는 RISC 마이크로프로세서인 Samsung S5PV210과 MOST Companion SoC인 OS85652

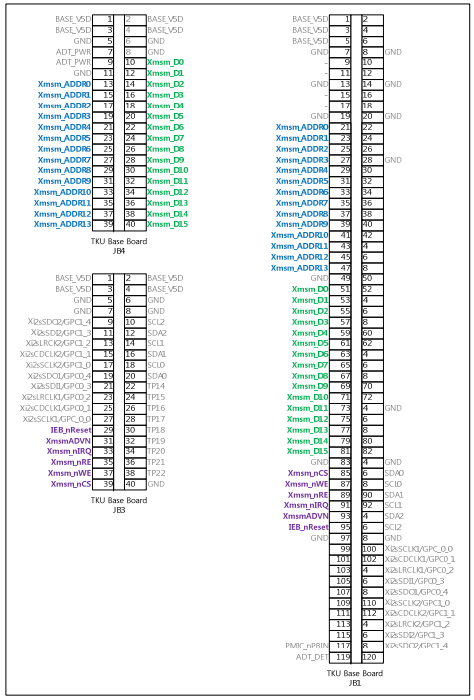
- Is Not finished Under Development!!!

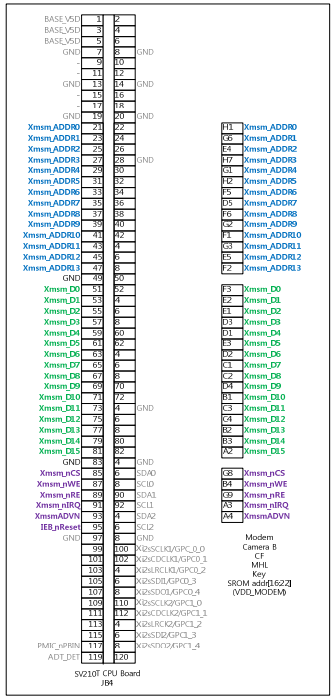
Hardware Architecture



Board connector pin

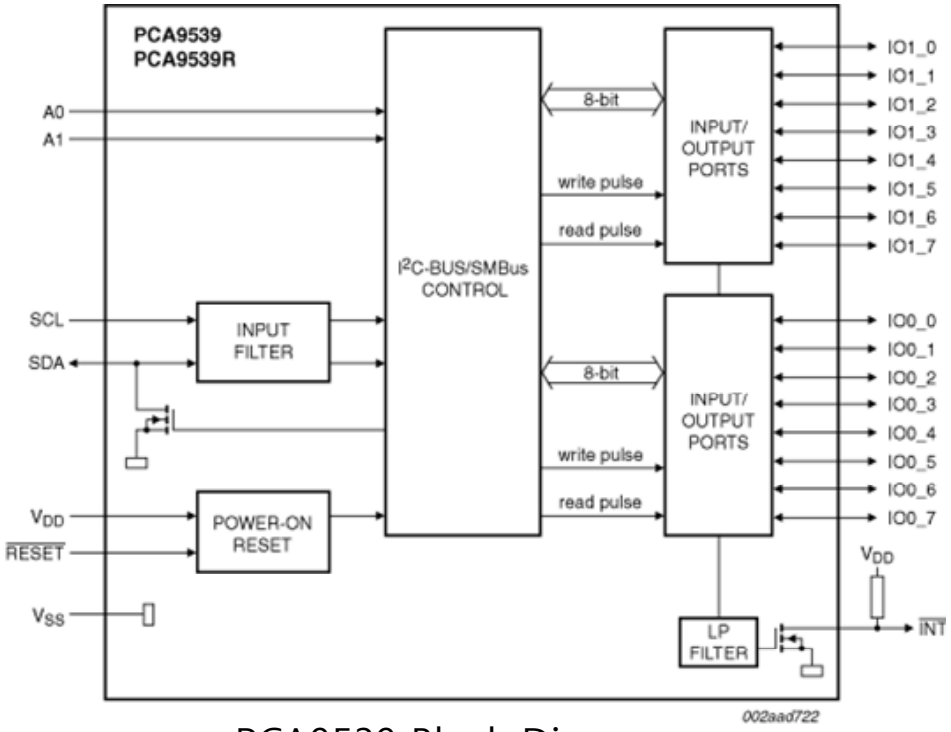




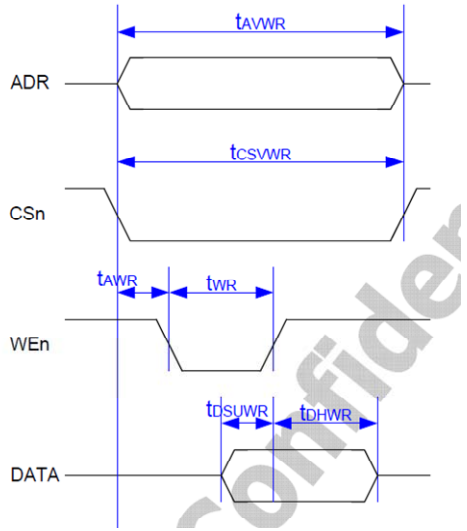


- C&D Platform Context Diagram (from MOST Low Level Driver SDS)

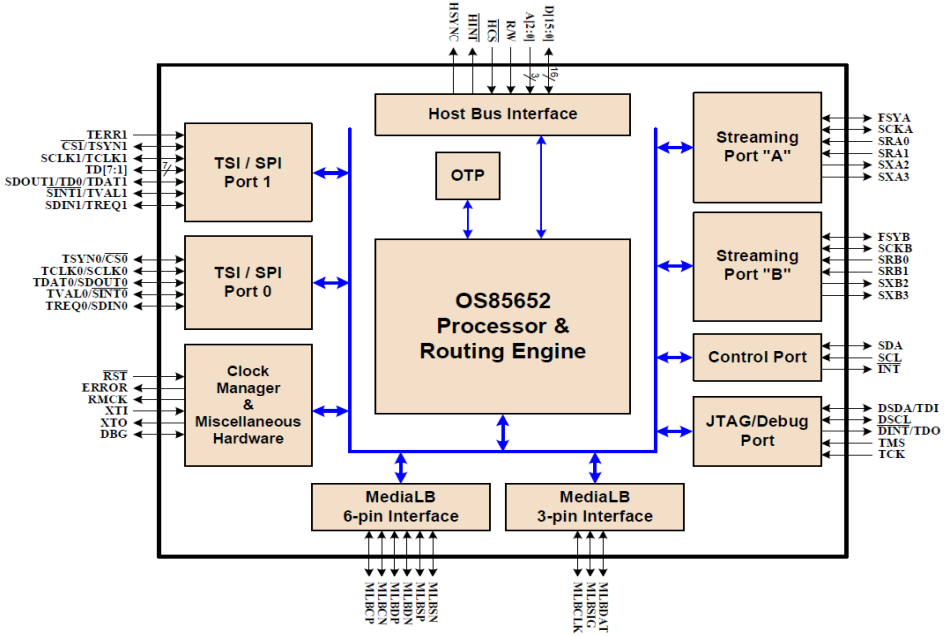
Interfaces



PCA9539 Block Diagram



OS85652 Physical Interfaces



- C&D Platform Context Diagram (from MOST Low Level Driver SIS)

Specific Software Requirements

Control

유스케이스 ID	UC1	
유스케이스 명	Control	
상세요구사항	001	송신
	002	수신

Isochronous

유스케이스 ID	UC3	
유스케이스 명	Asynchronous	
상세요구사항	001	송신
	002	수신
	003	Quadlet 단위로 대역폭 조정이 가능하다.

Asynchronous

유스케이스 ID	UC2	
유스케이스 명	Isochronous	
상세요구사항	001	송신
	002	수신
	003	송신과 수신 중 한 기능만 사용 가능하다.

Quality Attribute

영상 데이터의 크기는 480p 규격을 따른다.
WatchDog timer는 최대 500ms 로 이 시긴 이내에 최소한 한번 INIC 과 통신을 통해 INIC이 리셋되지 않도록 유지해야 한다.
MOST150 규격을 따라 48KHz 프레임 속도를 갖는다.

- C&D Platform Context Diagram (from MOST Low Level Driver SRS)

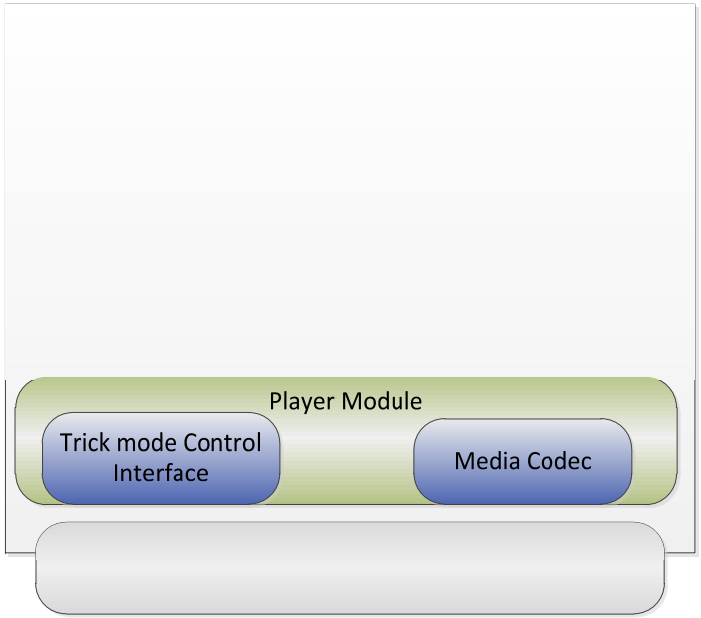
Low Level Driver Traceability Matrix

MLD SDS Traceability Matrix		Control	Isochronous	Asynchronous
Requrement Identifiers		UC1	UC2	UC3
Module Design				
1	Memory Access Function	x	x	x
2	Interrupt Function	x	x	x
3	Isochronous Channel Function		x	
4	Asynchronous Read Function			x
5	Asynchronous Write Function			x

MLD SIS Traceability Matrix		Control	Isochronous	Asynchronous
Requrement Identifiers		UC1	UC2	UC3
Hardware Interface				
1	Architecture	x	x	x
2	리셋 인터페이스	x		
3	OS85652와 INIC 간 인터페이스	x	x	x
4	S5PV210T CPU와 OS85652 인터페이스	x		
5	OS85652 Context	x	x	x

- C&D Platform Context Diagram (from MOST Low Level Driver Traceability Matrix)

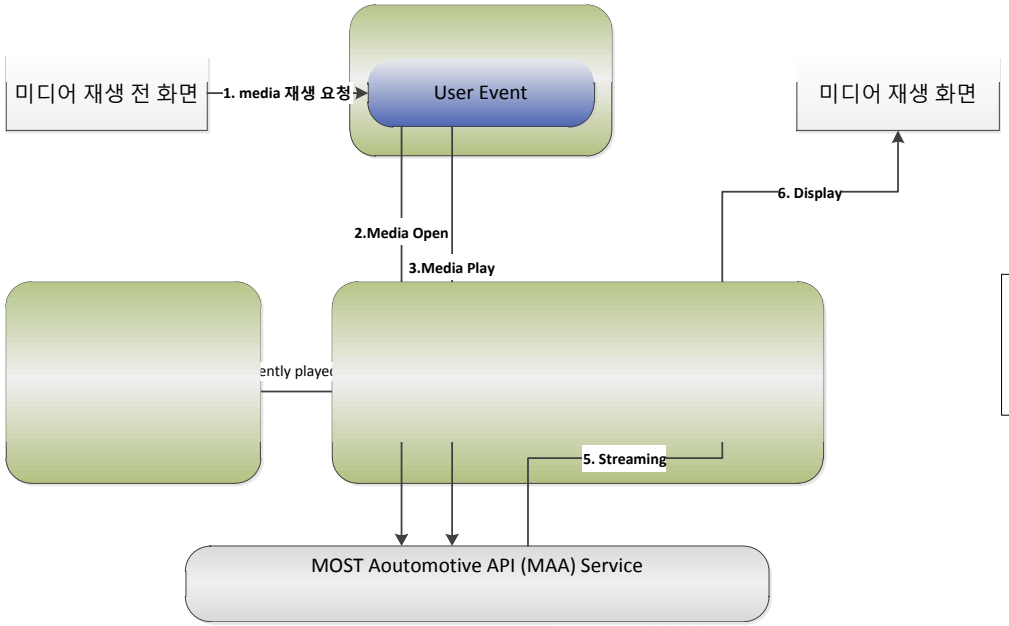
MOST Media Player Architecture

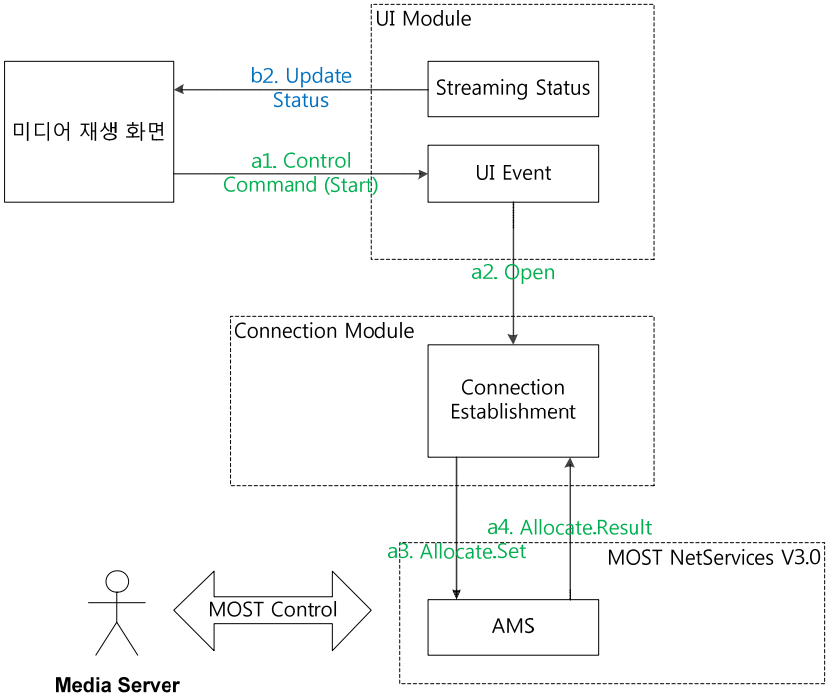


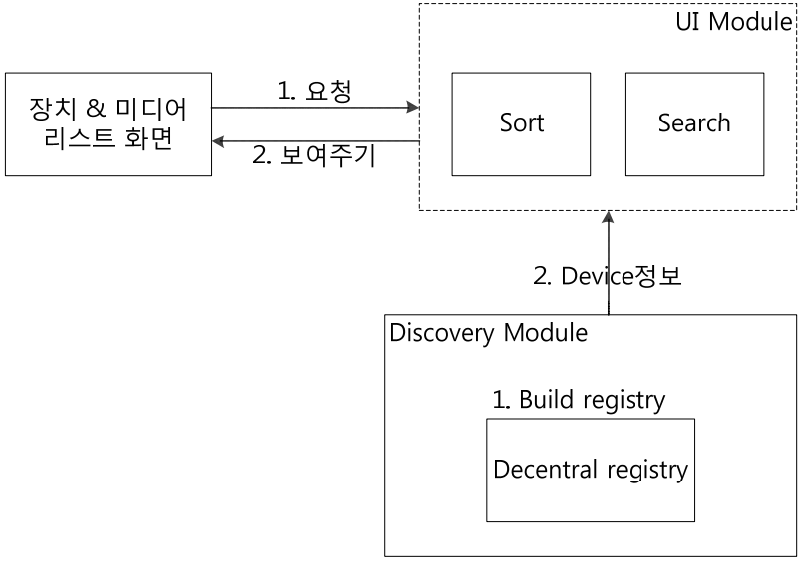
Module	Sub Module	설명
GUI	UIEvent	화면 전환 등 UI 내부에서 발생하는 Event에 대한 처리를 담당하는 모듈이다.
	UserEvent	Button Click 등 User가 UI를 통해 발생시키는 Event에 대한 처리를 담당하는 모듈이다.
Media List	Media List	사용자가 재생할 Media List를 생성하고 관리하는 모듈이다.
	Search	Media Search 기능을 담당하는 모듈이다.
Media Control	Trick mode control interface	미디어 재생을 제어하는 Action – 재생, 중지 등-을 Media codec에 전달하기 위한 interface를 담당하는 모듈이다.
	Media codec	사용자가 재생을 원하는 media data를 디코딩하는 모듈이다.

- C&D Platform Context Diagram (from MOST MediaPlayer SAS)

Media Playback Controls





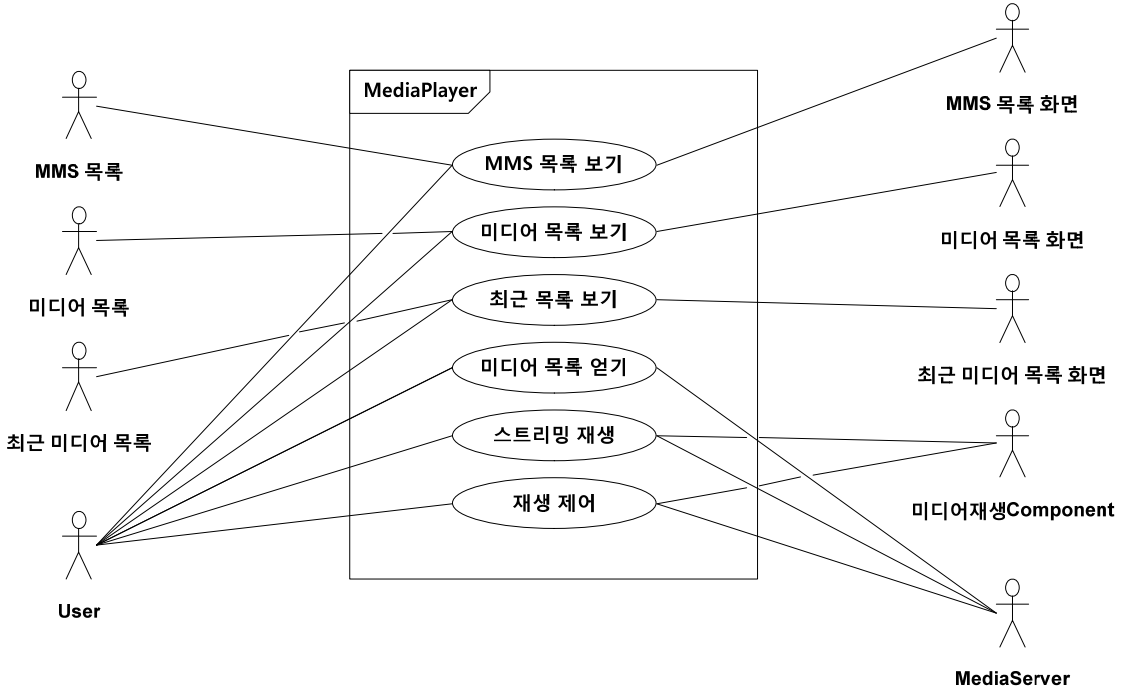


유스케이스 ID	SRS ID
CC-UC2	SRS-MMP-001~004

유스케이스 ID	SRS ID
CC-UC1	SRS-MMP-001~010
CC-UC6	SRS-MMP-001~002

- C&D Platform Context Diagram (from MOST MediaPlayer SDS)

Use Case Diagram



유스케이스 ID	CC-UC1	
유스케이스 명	스트리밍 재생	
상세요구사항	SRS-MMP-001	스트리밍 데이터를 재생한다.
	SRS-MMP-002	재생이 시작될 경우에는 재생 시작 버튼은 비활성화된다.
	SRS-MMP-003	재생하지 않는 상태에서는 재생 중지 버튼은 비활성화된다.
	SRS-MMP-004	미디어 파일이 선택되어 있지 않는 상태에서는 재생 제어 버튼들이 비활성화되는 기능을 제공한다.
	SRS-MMP-005	볼륨 조절이 제공된다.
	SRS-MMP-006	재생되는 상태를 시간 바 형태로 보여준다.
	SRS-MMP-007	스트리밍 데이터는 버퍼링을 후에 재생한다.
	SRS-MMP-008	스트리밍 데이터를 버퍼링하고 있는 동안에는 그 상태를 알려주기 위한 에니메이션을 보여준다.
	SRS-MMP-009	재생한 미디어 파일과 미디어 파일이 저장된 MediaServer의 정보를 최근 재생 목록에 추가한다.
	SRS-MMP-010	선택된 미디어 파일의 이름을 보여져야 한다.

- C&D Platform Context Diagram (from MOST MediaPlayer SRS)

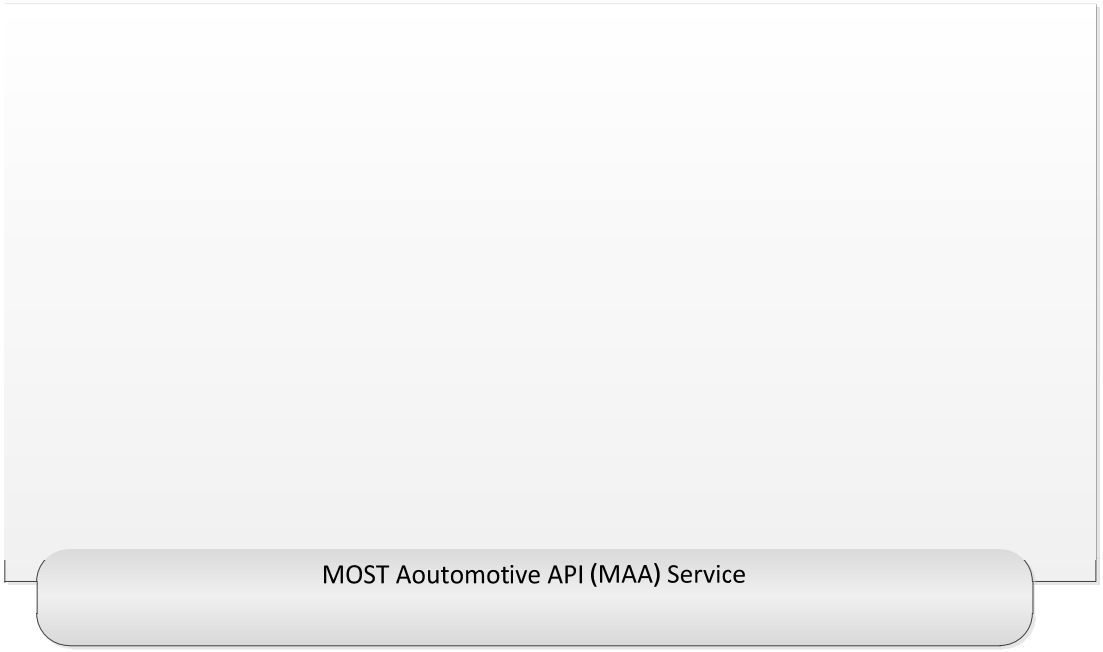
Media Player Traceability Matrix

MMP SAS Traceability Matrix	스트리밍 재생	MMS 목록 보기	미디어 목록 보기	최근 목록 보기	미디어 목록 얻기	재생 제어
Requrement Identifiers	CC-UC1	CC-UC2	CC-UC3	CC-UC4	CC-UC5	CC-UC6
Dynamic View Architecture						
1. Media list 조회		x	x		x	
2. 미디어 재생 제어	x					x
3. 최근 재생 목록				x		

MMP SIS Traceability Matrix	스트리밍 재생	MMS 목록 보기	미디어 목록 보기	최근 목록 보기	미디어 목록 얻기	재생 제어
Requrement Identifiers	CC-UC1	CC-UC2	CC-UC3	CC-UC4	CC-UC5	CC-UC6
Software Interface						
1. DiscoveryDevice		x				
2. DiscoveryMedia			x	x	x	
3. Streaming	x					
4. Media Player Control						x

- C&D Platform Context Diagram (from MOST MediaPlayer Traceability Matrix)

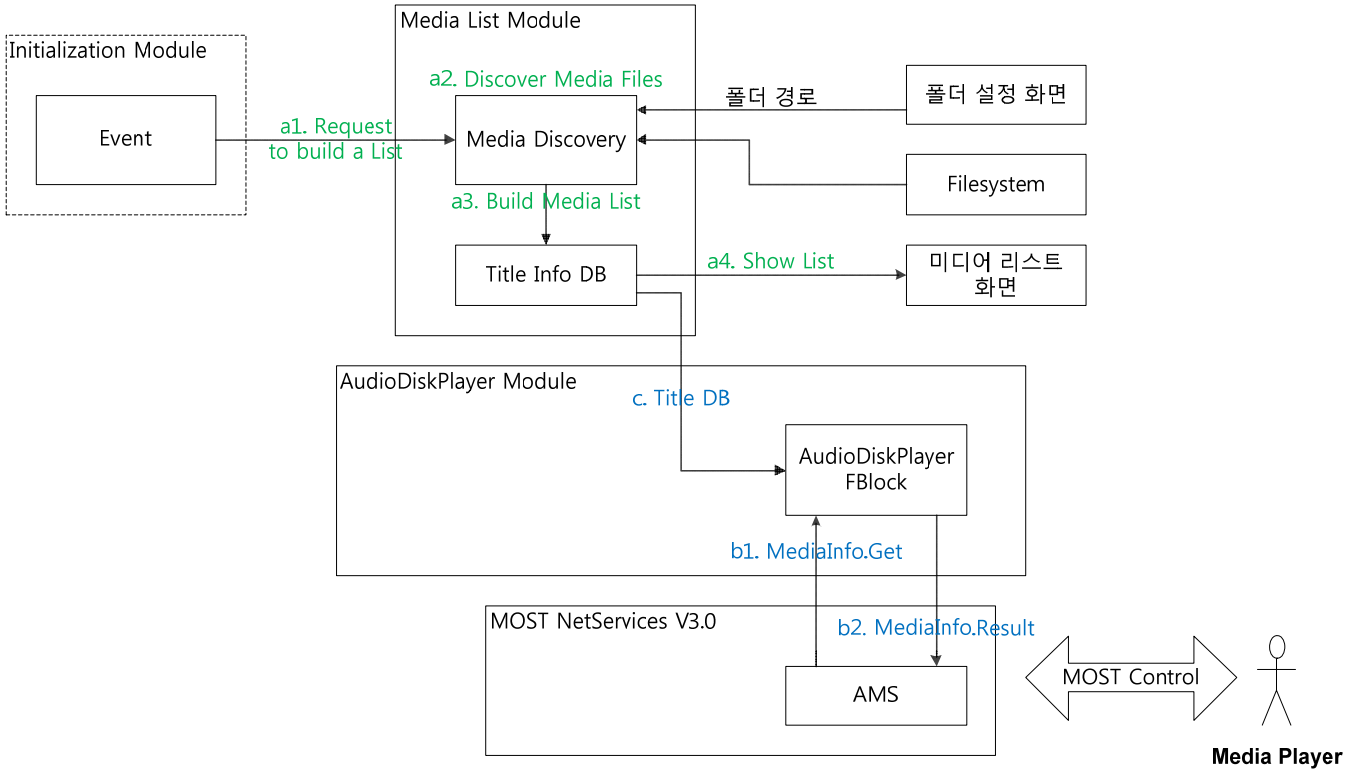
MOST Media Server Architecture



Module	Sub Module	설명
GUI	UIEvent	화면 전환 등 UI 내부에서 발생하는 Event에 대한 처리를 담당하는 모듈이다.
	UserEvent	Button Click 등 User가 UI를 통해 발생시키는 Event에 대한 처리를 담당하는 모듈이다.
Media List	Media Discovery	스트리밍할 대상의 Media를 찾는 모듈이다.
	Media info DB	찾은 Media 정보를 저장하는 DB 모듈

- C&D Platform Context Diagram (from MOST Media Server SAS)

Module Design



- C&D Platform Context Diagram (from MOST Media Server SDS)

Software Interface

Discovery Media

유스케이스 ID	SRS ID
CC-UC1	SRS-MMS-001 ~ 009
CC-UC2	SRS-MMS-001 ~ 004
CC-UC4	SRS-MMS-001

AddMediaInfo
Purpose: 미디어 파일 정보를 추가한다.
INPUT: MediaInfo
OUTPUT: N/A

RemoveMediaInfo
Purpose: 미디어 파일 정보를 삭제한다.
INPUT: MediaInfo
OUTPUT: N/A

ClearAllMedia
Purpose: 모든 미디어 파일 정보를 삭제한다.
INPUT: N/A
OUTPUT: N/A

GetMediaInfoList
Purpose: 미디어 파일 목록의 첫 번째 미디어 파일의 정보를 얻는다.
INPUT: N/A
OUTPUT: MediaInfo handle

NextMediaInfo
Purpose: 다음 미디어 파일 정보를 얻는다.
INPUT: MediaInfo handle
OUTPUT: MediaInfo handle

PrevMediaInfo
Purpose: 이전 미디어 파일 정보를 얻는다.
INPUT: MediaInfo handle
OUTPUT: MediaInfo handle

FindMediaInfo
Purpose: 입력된 정보를 바탕으로 미디어 파일을 찾는다.
INPUT: 검색 정보
OUTPUT: MediaInfo handle

Streaming

유스케이스 ID	SRS ID
CC-UC3	SRS-MMS-001 ~ 006
CC-UC5	SRS-MMS-001

Write
Purpose: 스트리밍 데이터를 송신한다.
INPUT: 스트리밍 데이터, 길이
OUTPUT: N/A

Connect
Purpose: 스트리밍을 요청한다.
INPUT: 대역폭 (Quadlet 개수)
OUTPUT: N/A

Disconnect
Purpose: 스트리밍을 종료한다.
INPUT: N/A
OUTPUT: N/A

- C&D Platform Context Diagram (from MOST Media Server SIS)

MOST Media Server Traceability Matrix

MMS SAS Traceability Matrix	미디어 목록 생성	미디어 목록 조회	스트리밍 상태 조회	미디어 목록 제공	스트리밍 전송
Requrement Identifiers	CC-UC1	CC-UC2	CC-UC3	CC-UC4	CC-UC5
Dynamic View Architecture					
1. 스트리밍할 대상 지정	x				
2. 스트림 미디어 정보 제공		x		x	
3. 스트림 상태 제공			x		x

MMS SIS Traceability Matrix	미디어 목록 생성	미디어 목록 조회	스트리밍 상태 조회	미디어 목록 제공	스트리밍 전송
Requrement Identifiers	CC-UC1	CC-UC2	CC-UC3	CC-UC4	CC-UC5
Communication Interface					
1. DiscoveryMedia	x	x		x	
2. Streaming			x		x

Module Design		미디어 목록 생성	미디어 목록 조회	스트리밍 상태 조회	미디어 목록 제공	스트리밍 전송
SSD-M-001	Generate MMS List	x				
SDS-M-002	Update MMS List		x	x		
SDS-M-003	Get Media List		x		x	
SDS-M-004	Generate Media List	x				
SDS-M-005	Set Media List	x				
SDS-M-006	Start Streaming					x
SDS-M-007	Transmit Streaming					x
SDS-M-008	Stop Streaming					x
SDS-M-009	Generate MOST Device List	x				
SDS-M-010	Statistics			x		

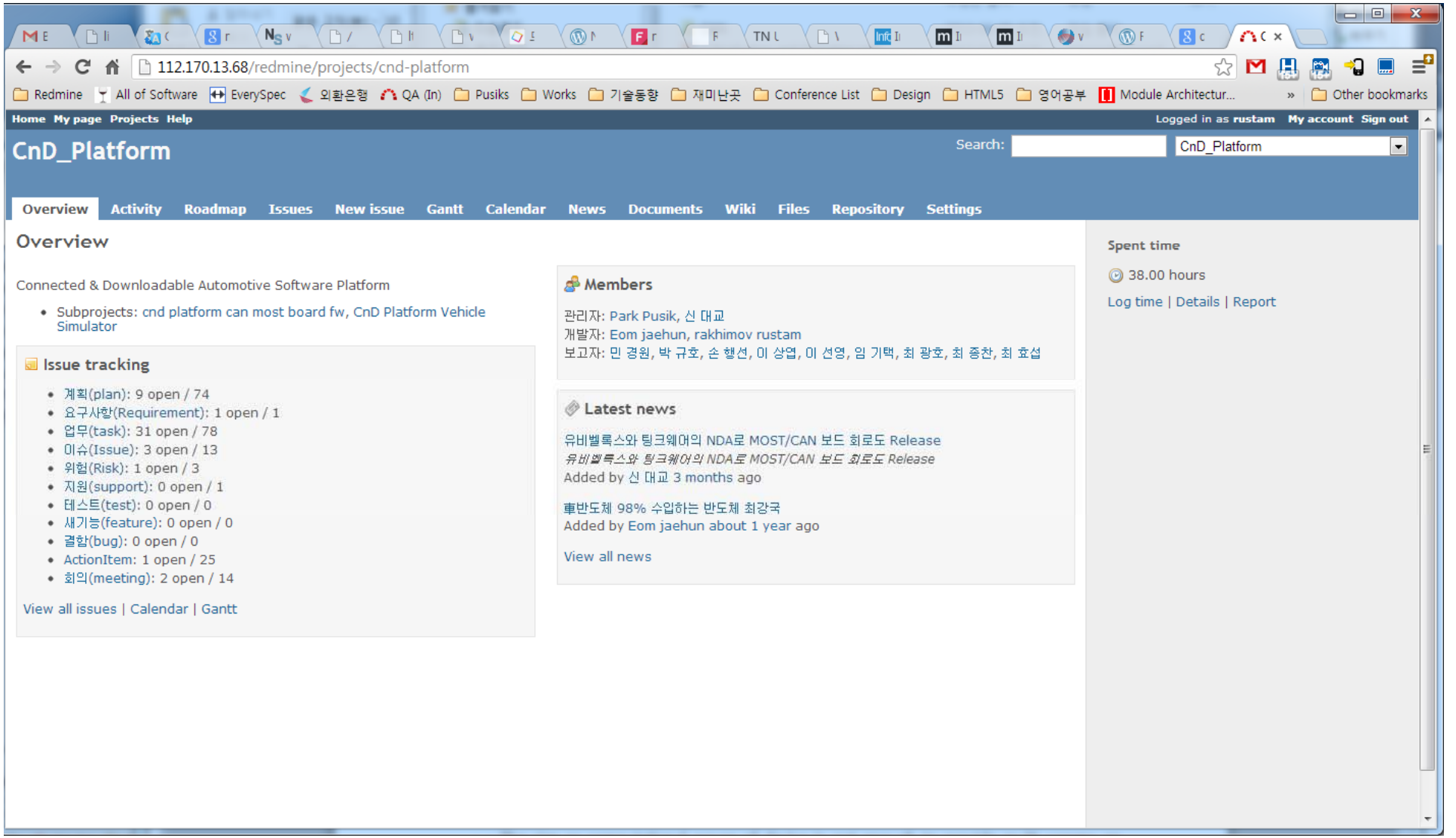
- C&D Platform Context Diagram (from MOST Media Server Traceability Matrix)

QA – Quality Assurance

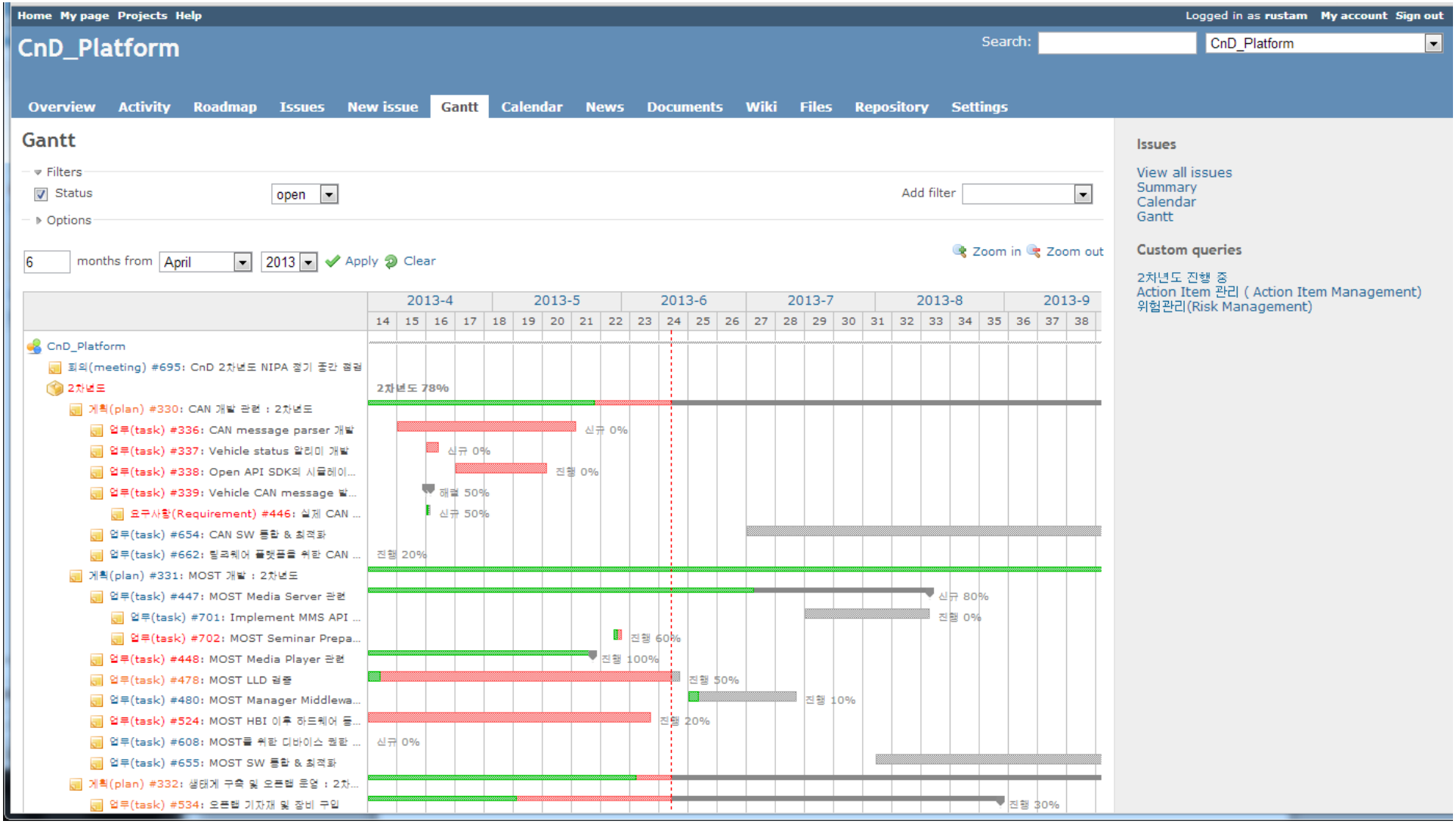
- Source Code
  - SVN

- Quality Management
  - Redmine

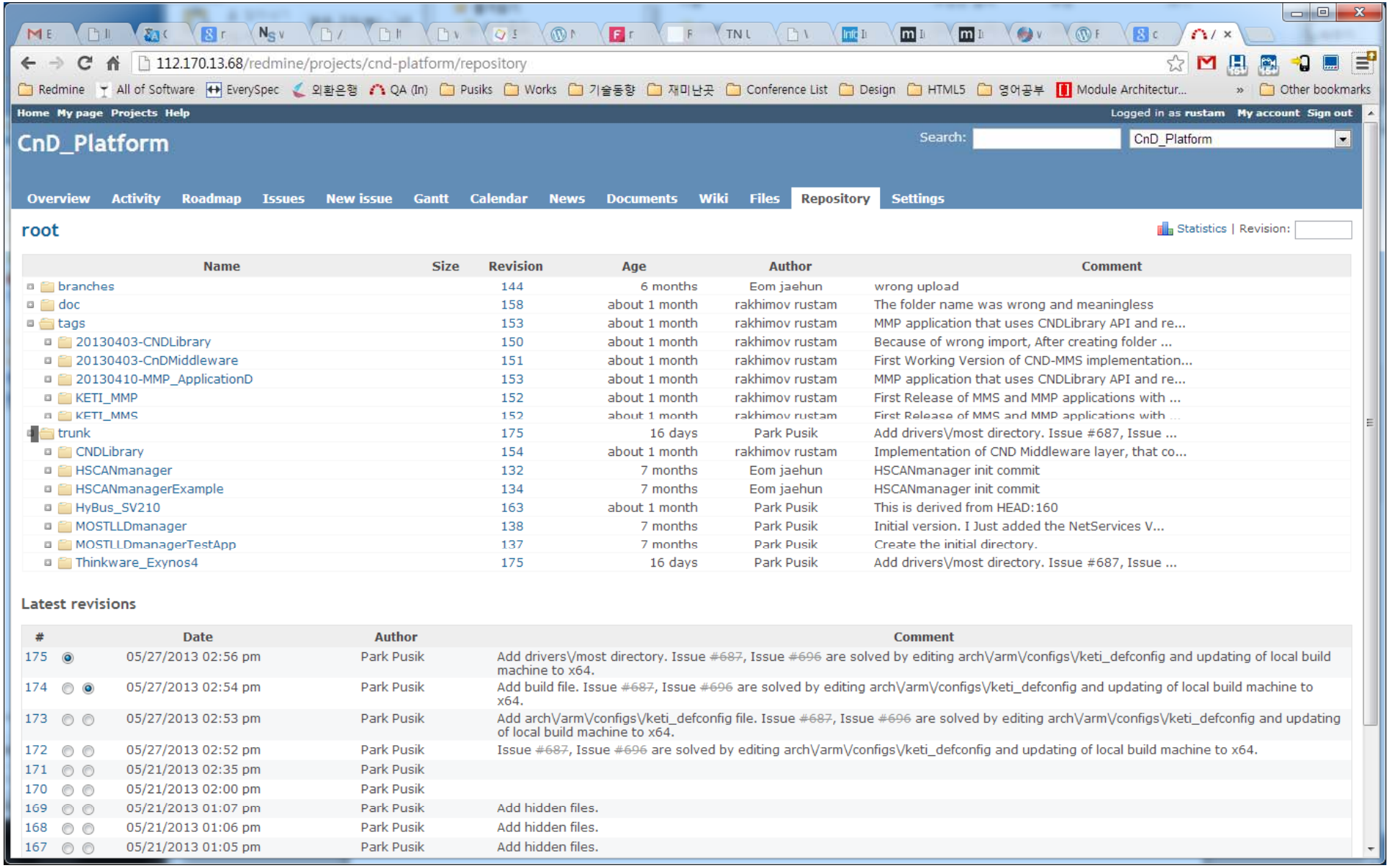
QA Overview


112.170.13.68/redmine/projects/cnd-platform
Redmine
All of Software
EverySpec
외환은행
QA (In)
Pusiks
Works
기술동향
재미난곳
Conference List
Design
HTML5
영어공부
Module Architectur...
Other bookmarks
Home My page Projects Help
Logged in as rustam My account Sign out
CnD_Platform
Search:
CnD_Platform
Overview Activity Roadmap Issues New issue Gantt Calendar News Documents Wiki Files Repository Settings
Overview
Connected & Downloadable Automotive Software Platform
Subprojects: cnd platform can most board fw, CnD Platform Vehicle Simulator
Issue tracking
계획(plan): 9 open / 74
요구사항(Requirement): 1 open / 1
업무(task): 31 open / 78
이슈(Issue): 3 open / 13
위험(Risk): 1 open / 3
지원(support): 0 open / 1
테스트(test): 0 open / 0
새기능(feature): 0 open / 0
결함(bug): 0 open / 0
ActionItem: 1 open / 25
회의(meeting): 2 open / 14
View all issues | Calendar | Gantt
Members
관리자: Park Pusik, 신 대교
개발자: Eom jaehun, rakhimov rustam
보고자: 민 경원, 박 규호, 손 행선, 이 상엽, 이 션영, 임 기택, 최 광호, 최 종찬, 최 효섭
Latest news
유비벨록스와 팅크웨어의 NDA로 MOST/CAN 보드 회로도 Release
유비벨록스와 팅크웨어의 NDA로 MOST/CAN 보드 회로도 Release
Added by 신 대교 3 months ago
車반도체 98% 수입하는 반도체 최강국
Added by Eom jaehun about 1 year ago
View all news
Spent time
38.00 hours
Log time | Details | Report

QA (Gantt Diagram)

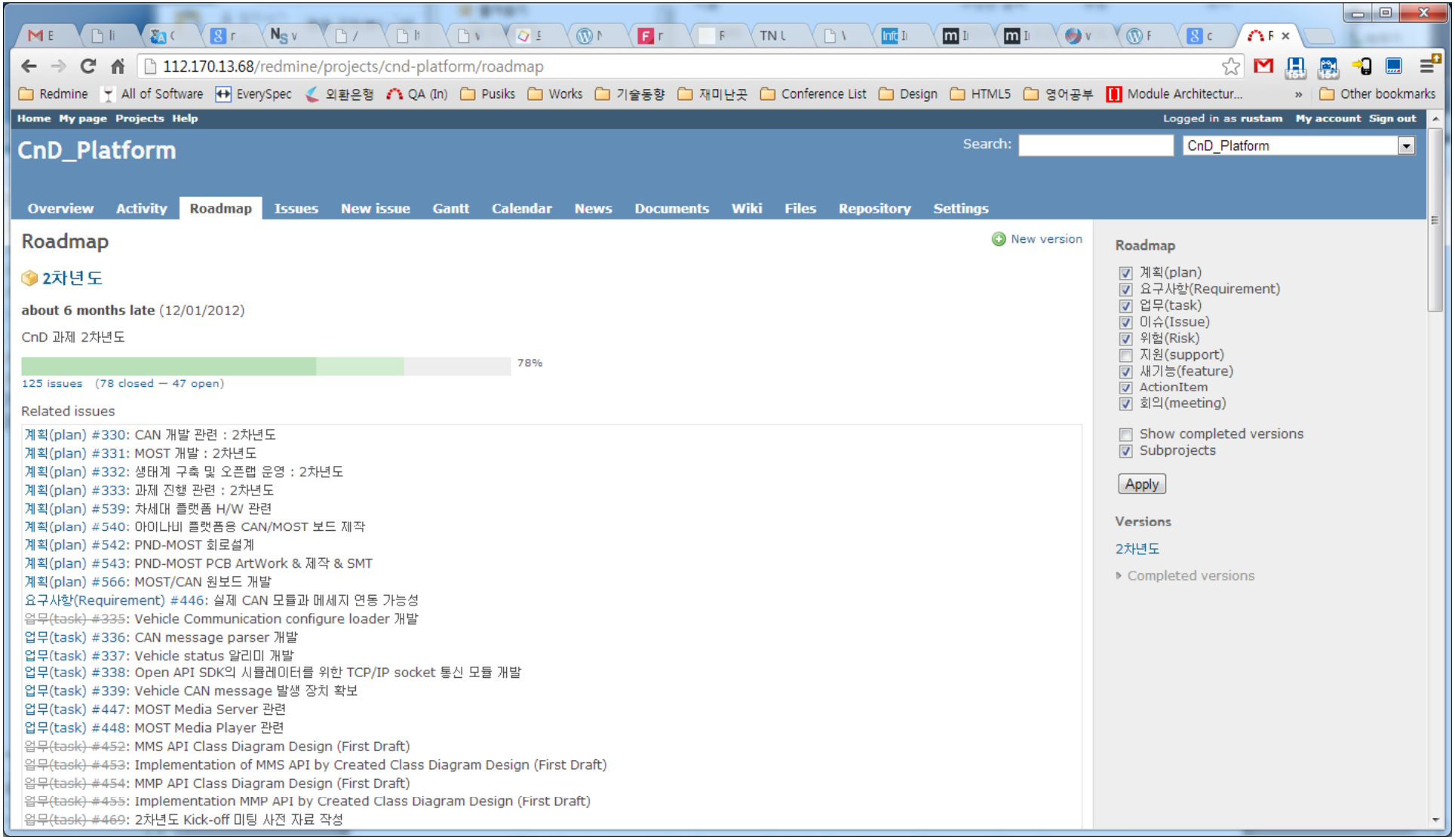


QA (Repository View)



- Repository is Synchronized with SVN Server

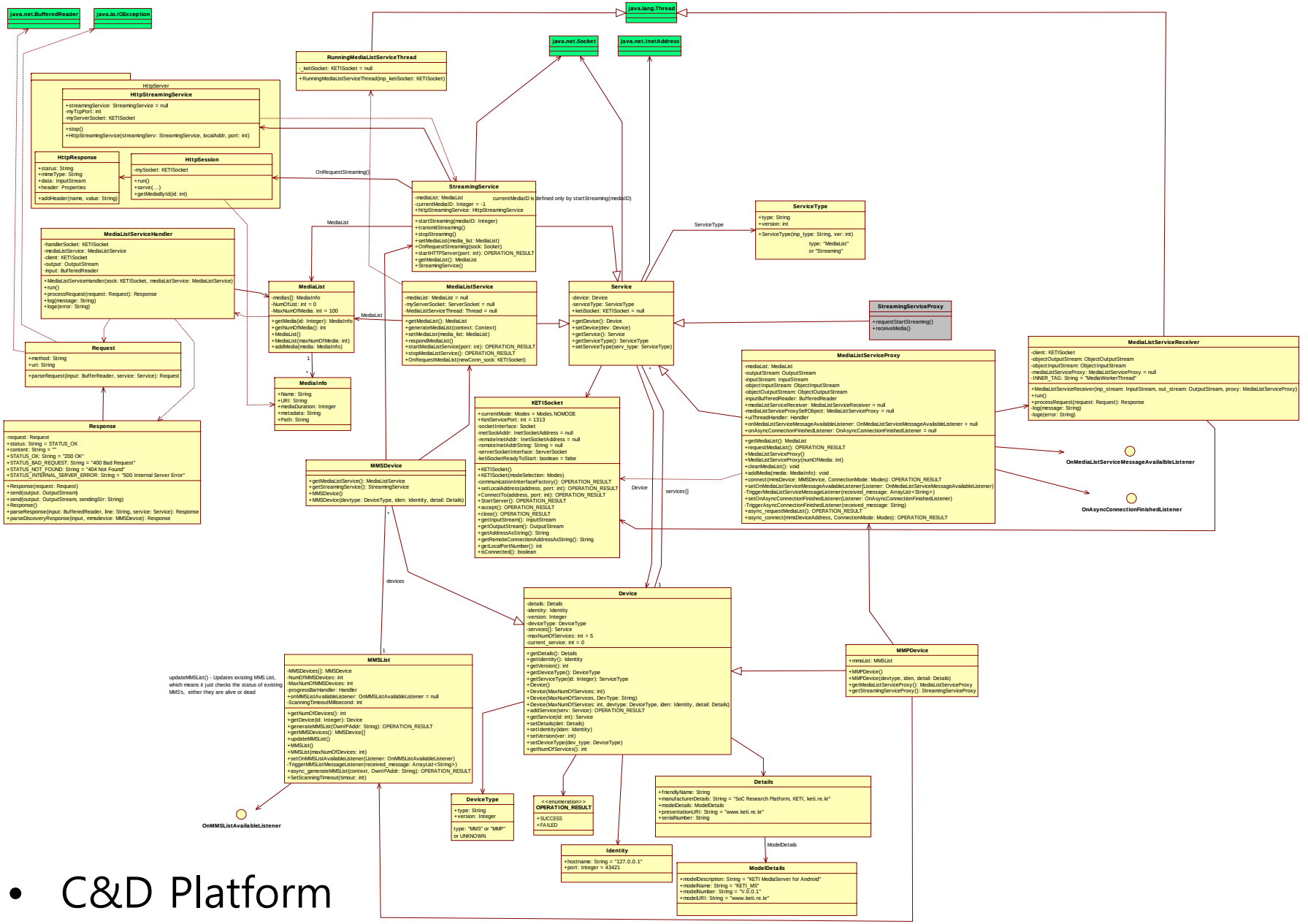
QA Roadmap


112.170.13.68/redmine/projects/cnd-platform/roadmap
Redmine
All of Software
EverySpec
외환은행
QA (In)
Pusiks
Works
기술동향
재미난곳
Conference List
Design
HTML5
영어공부
Module Architectur...
Other bookmarks
Home My page Projects Help
Logged in as rustam My account Sign out
CnD_Platform
Search:
CnD_Platform
Overview Activity Roadmap Issues New issue Gantt Calendar News Documents Wiki Files Repository Settings
Roadmap
New version
2차년도
about 6 months late (12/01/2012)
CnD 과제 2차년도
78%
125 issues (78 closed — 47 open)
Related issues
계획(plan) #330: CAN 개발 관련 : 2차년도
계획(plan) #331: MOST 개발 : 2차년도
계획(plan) #332: 생태계 구축 및 오픈랩 운영 : 2차년도
계획(plan) #333: 과제 진행 관련 : 2차년도
계획(plan) #539: 차세대 플랫폼 H/W 관련
계획(plan) #540: 아이나비 플랫폼용 CAN/MOST 보드 제작
계획(plan) #542: PND-MOST 회로설계
계획(plan) #543: PND-MOST PCB ArtWork & 제작 & SMT
계획(plan) #566: MOST/CAN 원보드 개발
요구사항(Requirement) #446: 실제 CAN 모듈과 메세지 연동 가능성
업무(task) #335: Vehicle Communication configure loader 개발
업무(task) #336: CAN message parser 개발
업무(task) #337: Vehicle status 알리미 개발
업무(task) #338: Open API SDK의 시뮬레이터를 위한 TCP/IP socket 통신 모듈 개발
업무(task) #339: Vehicle CAN message 발생 장치 확보
업무(task) #447: MOST Media Server 관련
업무(task) #448: MOST Media Player 관련
업무(task) #452: MMS API Class Diagram Design (First Draft)
업무(task) #453: Implementation of MMS API by Created Class Diagram Design (First Draft)
업무(task) #454: MMP API Class Diagram Design (First Draft)
업무(task) #455: Implementation MMP API by Created Class Diagram Design (First Draft)
업무(task) #469: 2차년도 Kick-off 미팅 사전 자료 작성
Roadmap
계획(plan)
요구사항(Requirement)
업무(task)
이슈(Issue)
위험(Risk)
지원(support)
새기능(feature)
ActionItem
회의(meeting)
Show completed versions
Subprojects
Apply
Versions
2차년도
Completed versions

SWDP(Software Development Plan)

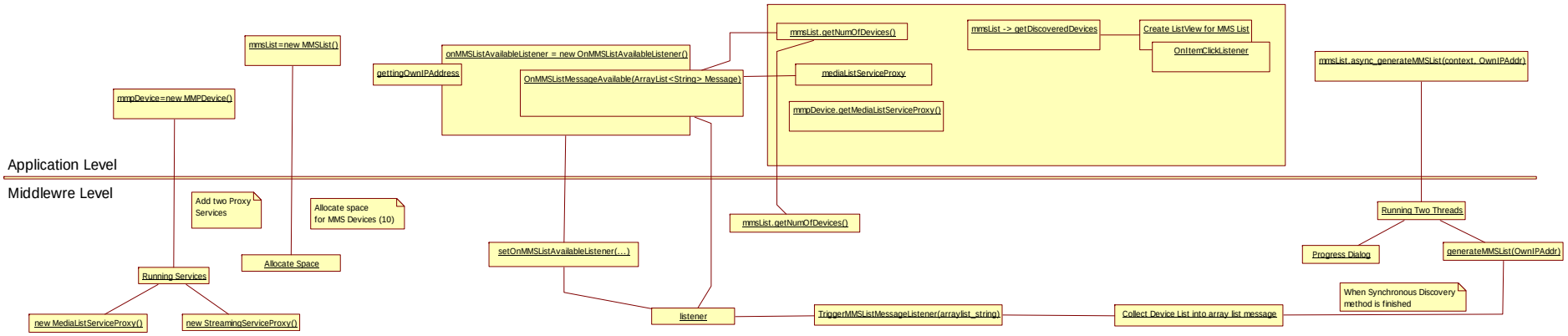
- Environment
  - Windows XP, Ubuntu Linux, MacOS
  - Java Virtual Machine
  - QNX Neutrino Real Time Operating System(RTOS)
- Development Language
  - Java, C/C++, Verilog (For the Hardware)
- Tools
  - Android SDK
  - Atmel Developer Toolset
  - ModelSIM
  - Xilinx Tools

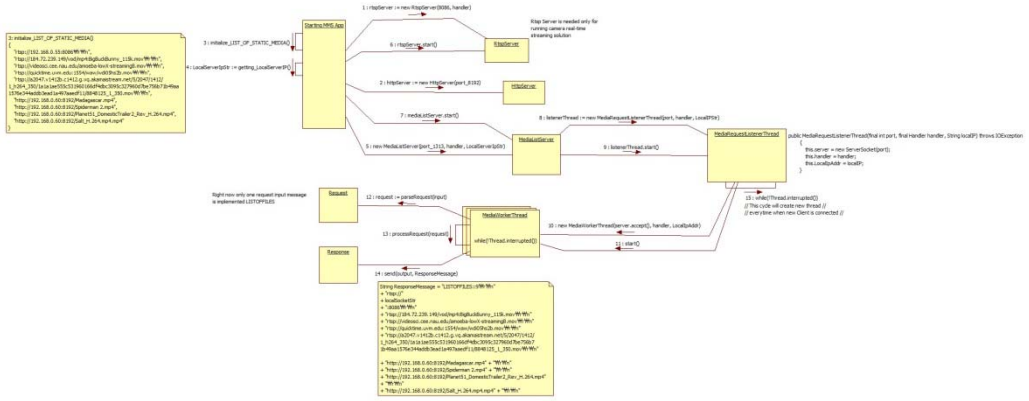
UML Diagram (MOST API)

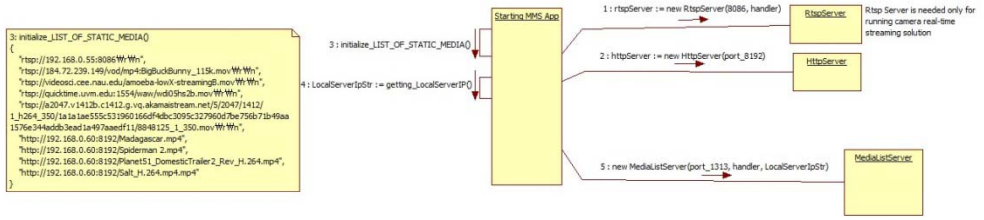


- C&D Platform

Interaction Sequence Diagram





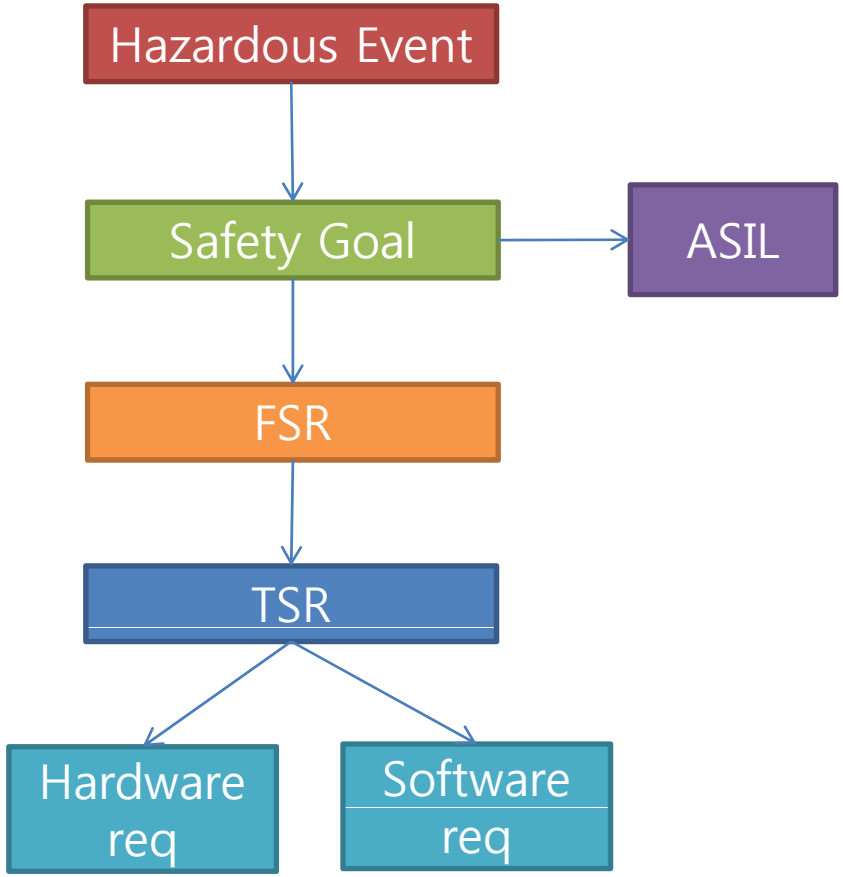


- C&D Platform

Adding Safety Requirements

Safety Goal

- Definition of hazard event is important
- Safety Goal is derived from hazardous event
- Using Safety Goal the ASIL level can be assigned. (That way Hazardous event can get assigned ASIL level)
- FSRs are derived from Safety Goals
- FSRs are implemented by TSRs (Technical Safety Requirement)
- Each TSR can then be implemented by a Software or Hardware requirement (it is quite low level)



Safety Requirements

6.4.1.1 To achieve the characteristics of safety requirements listed in 6.4.2.4, safety requirements shall be specified by an appropriate combination of:

a) natural language, and

b) methods listed in Table 1.

NOTE For higher level safety requirements (e.g. functional and technical safety requirements) natural language is more appropriate while for lower level safety requirements (e.g. software and hardware safety requirements) notations listed in Table 1 are more appropriate.

Table 1 — Specifying safety requirements

Methods		ASIL			
		A	B	C	D
1a	Informal notations for requirements specification	++	++	+	+
1b	Semi-formal notations for requirements specification	+	+	++	++
1c	Formal notations for requirements specification	+	+	+	+

++ indicates that the method is highly recommended for the identified ASIL;
+ indicates that the method is recommended for the identified ASIL;
o indicates that the method has no recommendation for or against its usage for the identified ASIL.

Safety Related Notes

- Requirements represented in Natural Language should be translated into Formal or Semi-formal methods

- A major part of the complexity is that the FSC (Functional Safety Concept) “should” be represented as a tree or graph that maps safety goals to functional safety requirements in a process of hierarchical decom position Ref

Example: Natural language Requirements

While <the vehicle fuel level> *is less than the* <low fuel level threshold> *the* <fuel level display system> *shall* <present> <the low fuel level warning> *to* <the driver>

- Requirements can be specified in constrained natural language CNL
- Metrics by Kaiya and Saeki
  - Correctness
  - Completeness
  - Consistency
  - Unambiguity
- Requirement metrics in DODT
  - Completeness
  - Inconsistency
  - Ambiguity
  - Noise
  - Opacity
  - Redundancy

Item Definition: Safety Related

Safety Related Requirements in natural language

ID	Requirement Text
REQ0	Danger or Alarm Messages on the Road have a highest priority. They should be louder than any other sounds
REQ1	Incoming phone call, is second priority, since the call might represent important messages to the user
REQ2	Navigation System is the third priority, since it navigates to the goal

Some of the Possible Danger Alarms related inside the car

Alarms	Description
Seat Belt	Seat belt is not fixed
Child Car Seat Alarm	Alarms related to Childs seat
Doors are not closed	
Driver Felling a Sleep	
Avoid eye from the Road	May be for phone call or look somewhere else

Assign ASIL Level

- Follow to the ISO-26262:3. Hazard analysis and risk assessment. Annex B
- Define
  - Severity
  - Probability of Exposure
  - Controllability

Assign ASIL Level (Severity)

- To Define severity it is better to follow AIS (AIS-represents a categorization of injury classes)
  - AIS 0: no injuries;
  - AIS 1: light injuries such as skin-deep wounds, muscle pains, whiplash, etc.;
  - AIS 2: moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures, etc.;
  - AIS 3: severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing, etc.;
  - AIS 4: severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing
  - AIS 5: critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding;
  - AIS 6: extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities), etc.

Alarms	Description
Seat Belt	Seat belt is not fixed
Child Car Seat Alarm	Alarms related to Childs seat
Doors are not closed	
Driver Felling a sleep	
Avoid eye from the Road	May be for phone call or look somewhere else

Assign ASIL Level (Severity)

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	— AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6

- S2 can be assigned for Severity

Assign ASIL Level

(Probability of Exposure)

- An estimation of the probability of exposure requires the evaluation of the scenarios
- E0 is assigned to situations which are considered to be unusual or incredible. Example (From ISO-26262:3 AnnexB):
  - a very unusual, or infeasible, co-occurrence of circumstances
    - a vehicle involved in an accident with another vehicle that is carrying a hazardous material (note this does not apply to a vehicle which is designed to carry that material);
    - a vehicle involved in an incident which includes an airplane landing on a highway
  - natural disasters, e.g. earthquake, hurricane, forest fire
- Real World Examples for E0
  - (Russia) http://www.youtube.com/watch?feature=endscreen&v=P0GQfwynpyE&NR=1
  - (South Korea) http://www.youtube.com/watch?v=nzCeyTdO_zY

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time

Alarms	Description
Seat Belt	Seat belt is not fixed
Child Car Seat Alarm	Alarms related to Childs seat
Doors are not closed	
Driver Felling a sleep	
Avoid eye from the Road	May be for phone call or look somewhere else

- E4 can be assigned for Exposure level

Assign ASIL Level (Controllability)

Chances to avoid harm

- The determination of the controllability class, for a given hazard, requires an estimation of the probability that the representative driver will be able to retain or regain control of a vehicle if a given hazard were to occur

Driving factors and scenarios	Class of controllability (see Table 3)			
	C0	C1	C2	C3
	Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted as adequate: "Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven. This is appropriate evidence of the rationale for a C2-estimate.

Alarms	Controllability
Seat Belt	90%
Child Car Seat Alarm	60%
Doors are not closed	85%
Felling a sleep	90%
Avoid eye from the Road	95%

84%

- C2 can be assigned for Controllability

Assign ASIL Level

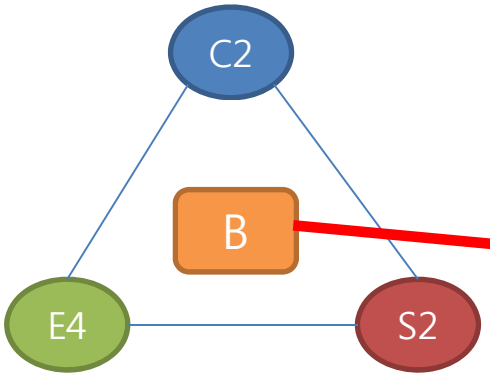
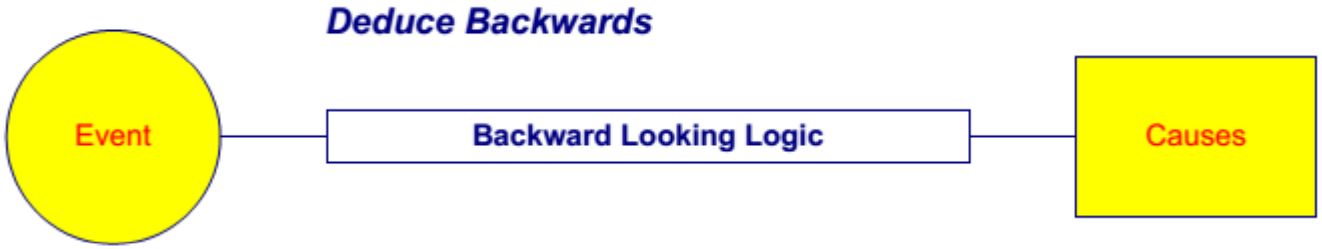


Table 4 — ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

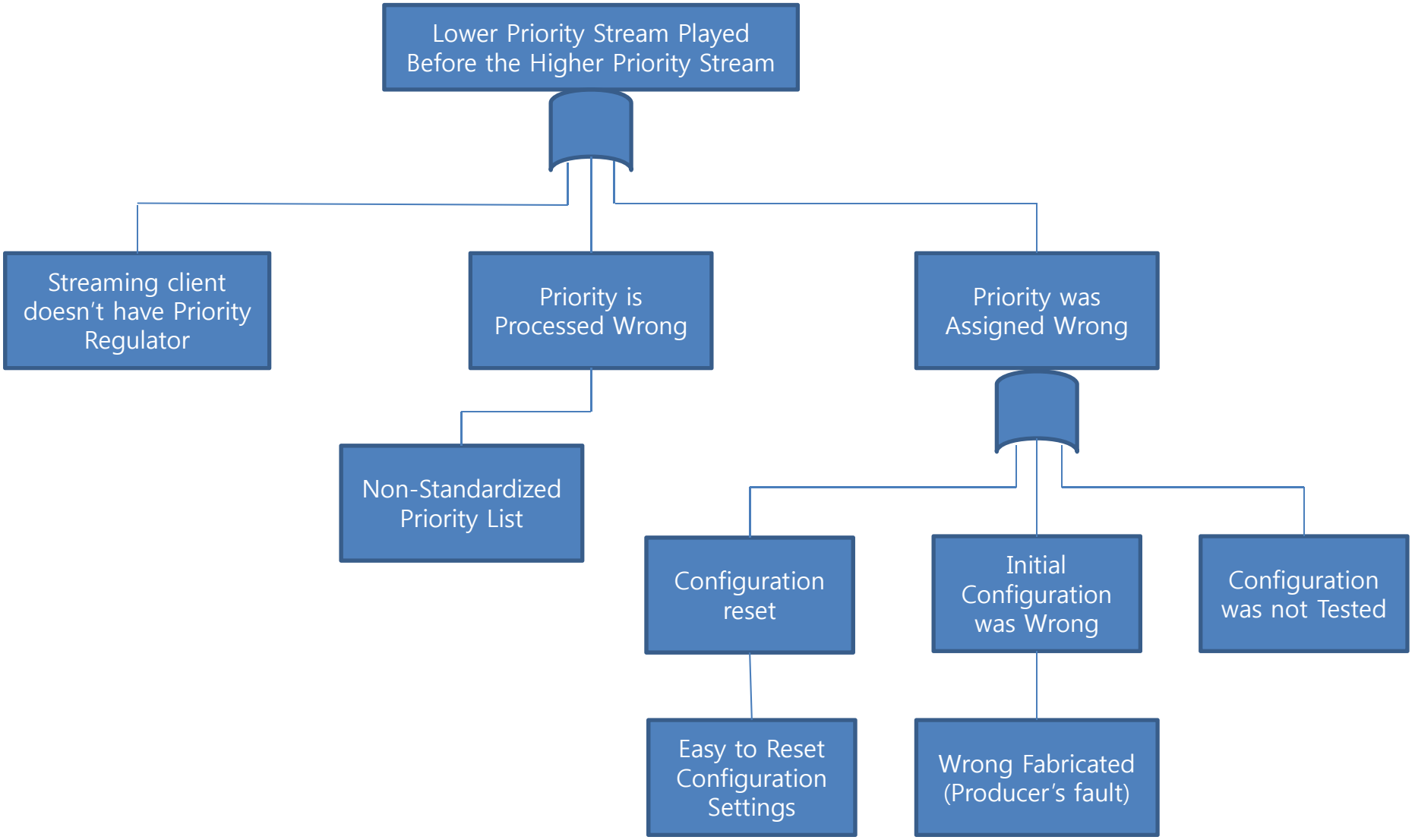
- ASIL Level B is assigned

FTA Analysis



- Fault tree analysis (FTA) is a top down, Deductive reasoning failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events.

FTA (Fault Tree Analysis)



- Fault Tree Analysis

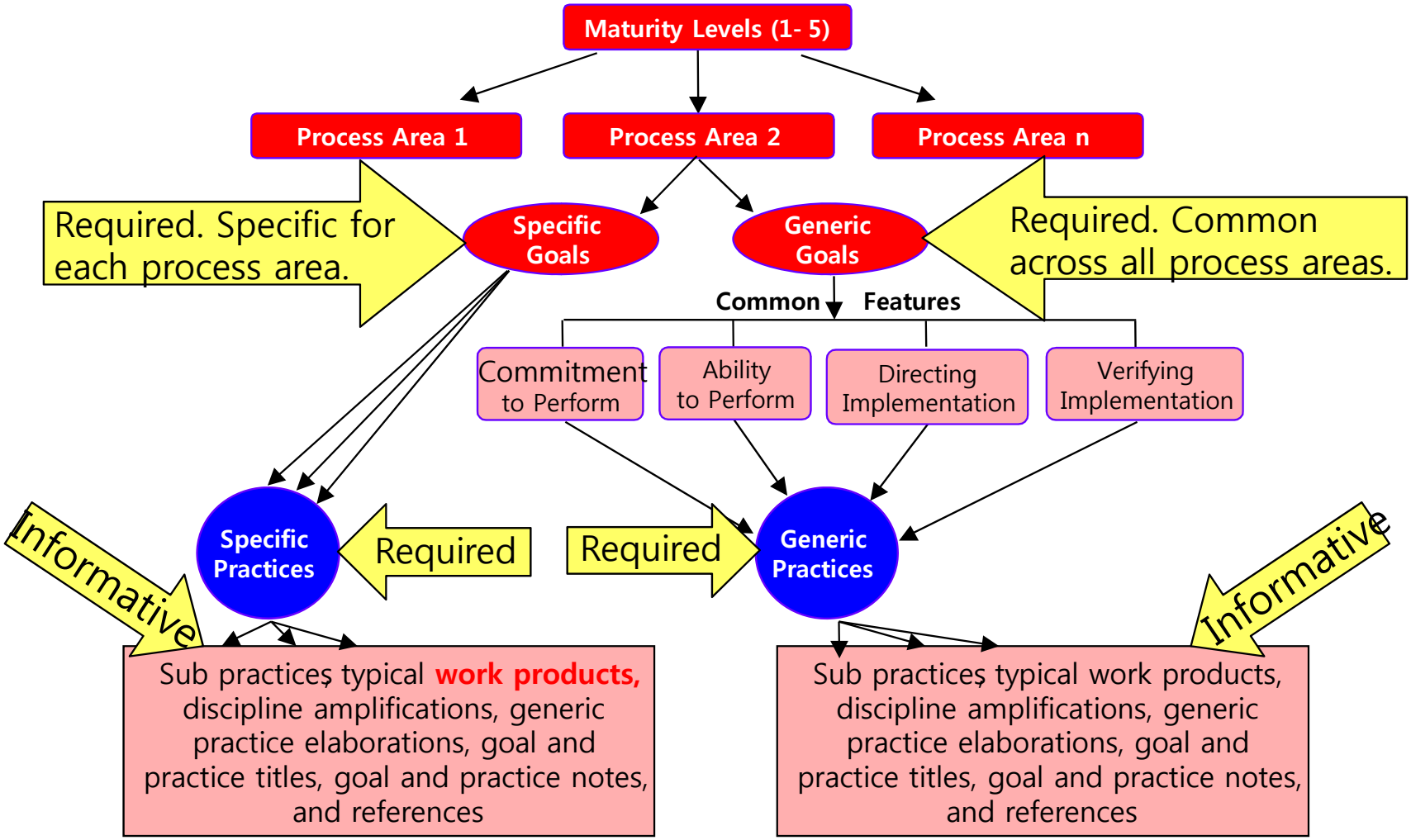
There can be Two Solutions

- Hardware Module that controls Priority of the Streams. To do that Timing Master and Connection Master should be studied. It could give a result. Originally Timing Master can control priority of the streams, but it is little complicated.

- Software solution could be easily designed and implemented. It means the implementation will held on higher level. To do that new Priority Controller [or Priority Regulator] component should be added.
  - It checks prioritized channels for triggering any alarm message. When the stre aming received from high prioritized channel it will be set on main stream

- C&D Platform

CMMi Terminology & Structure



CMMI (Capability Levels)

- Capability Level 1: The organization achieves the specific goals of the respective process area(s)
- Capability Level 2: The organization institutionalizes a managed process for the respective process area(s)
- Capability Level 3: The organization institutionalizes a defined process for the respective process area(s)

Institutionalize - To make part of a structured and usually well-established system

Generic Goals & Practices

- Each process area is defined by a set of goals and practices
- Generic goals and practices: They are part of every process area

- Generic Practices by Goal
- GG 1 Achieve Specific Goals
  - ✓ GP 1.1 Perform Specific Practices

Generic Goals & Practices

- GG 2 Institutionalize a Managed Process
  - ✓ GP 2.1 Establish an Organizational Policy
  - ✓ GP 2.2 Plan the Process
  - ✓ GP 2.3 Provide Resources
  - ✓ GP 2.4 Assign Responsibility
  - ✓ GP 2.5 Train People
  - ✓ GP 2.6 Manage Configurations (Place selected work products of the process under appropriate levels of control)
  - ✓ GP 2.7 Identify and Involve Relevant Stakeholders ???
  - ✓ GP 2.8 Monitor and Control the Process
  - ✓ GP 2.9 Objectively Evaluate Adherence
  - ✓ GP 2.10 Review Status with Higher Level Management

Generic Goals & Practices

- GG 3 Institutionalize a Defined Process
  - ✓ GP 3.1 Establish and maintain the description of a defined process
  - ✓ GP 3.2 Collect Improvement Information
- GG 4 Institutionalize a Quantitatively Managed Process
  - ✓ GP 4.1 Establish Quantitative Objectives for the Process
  - ✓ GP 4.2 Stabilize subprocess Performance
- GG 5 Institutionalize an Optimizing Process
  - ✓ GP 5.1 Ensure Continuous Process Improvement
  - ✓ GP 5.2 Correct Root Causes of Problems

Missing !

Institutionalization is really about how the processes are performed, how they're managed, how they're defined, what to measure and control the processes, and how they're continuously improving

Some Facts about CMMI

- CMMI Maturity Level 2 process areas are more broadly applicable to the immediate needs of project rather than Maturity level 3
- As higher maturity level you climb, the process areas become less and less applicable

CMMi Process Areas

Maturity Level	Project Management	Engineering	Process Management	Support
5 (Optimizing)			~~Organizational Innovation & Deployment~~	~~Causal Analysis & Resolution~~
4 (Quantitatively Managed)	~~Quantitative Project Management~~		~~Organizational Process Performance~~	
3 (Defined)	~~Integrated Project Mngt~~	Requirements Development	Organizational Process Focus	~~Decision Analysis & Resolution~~
	~~Risk Management~~	Technical Solution	Organizational Process Definition	
		Product Integration	Organizational Training	
		Verification		
		Validation		
2 (Managed)	Project Planning	Requirements Management		Measurement & Analysis
	Project Monitoring & Control			Process & Product Quality Assurance
	Supplier Agreement Management			Configuration Management
1 (Initial)				

V & V

- ATMEL and all Related development tools are used

- Why ATMEL is ok for 26262: http://www.atmel.com/Images/Atmel-4073-AVR-Microcontrollers-for-Automotive_Brochure.pdf

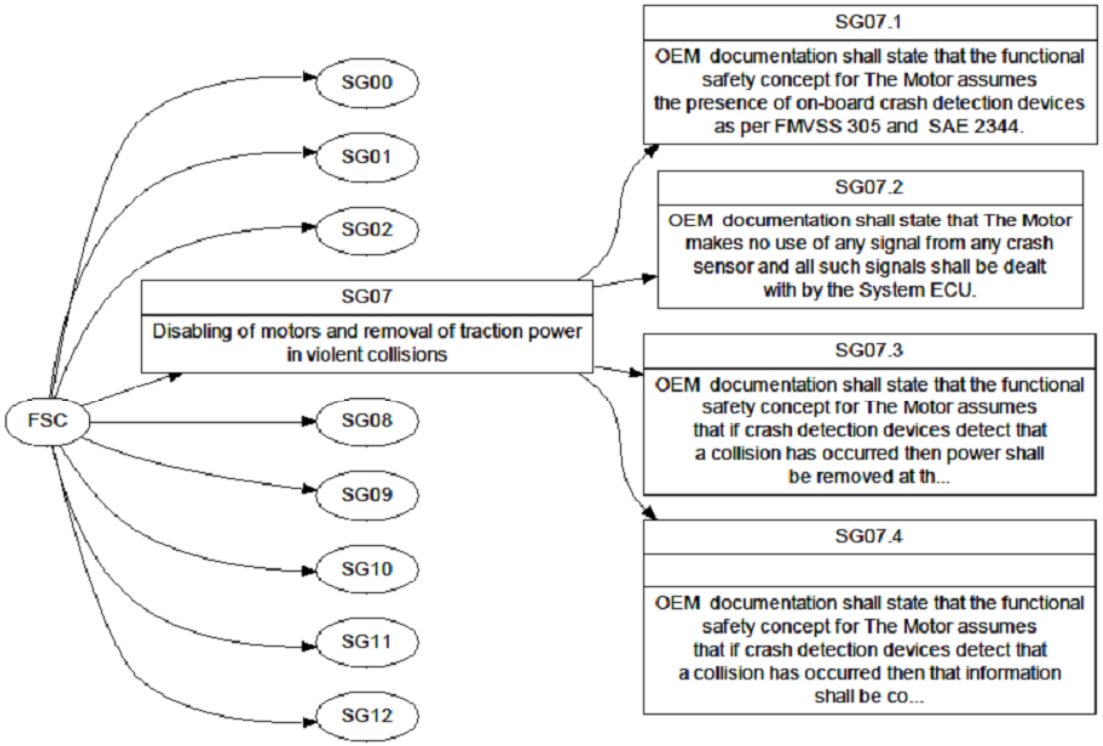
- One Remark:
  - Third Party jtag from seniorcom, not checked for ISO 26262. http://www.seniorcom.co.kr/

Thank You

ISO 26262: EXPERIENCE APPLYING PART 3 TO AN IN-WHEEL ELECTRIC MOTOR

M. Ellims, H. Monkhouse, A. Lyon

Protean Electric Ltd, UK, Mike.Ellims/Helen.Monkhouse@proteanelectric.com



4.7 Functional safety concept

Development of the FSC from the safety goals formulated during the Scenario Identification and Hazard Classification process is not particularly straight forward. A major part of the complexity (possibly self inflicted) is that the FSC "should" be represented as a tree or graph that maps safety goals to functional safety requirements in a process of hierarchical decomposition as shown in Figure 2 of clause 8 [3].

For the wheel motor this logical structure was represented as a tree within a spreadsheet, where high level goals were decomposed into sub-goals and then into functional safety requirements. The hierarchy of this structure was created following the derivation of the safety requirements. This process is quite straight forward if only the top level safety goals and requirements directly derived from those goals are considered.

- Back

Good Resources and related works

- According to the UPPSALA Universitet "Unambiguous requirements in Functional safety and ISO 26262: dream or reality?" Patrik Sternudd
  The most relevant source regarding requirements in ISO 26262 is Part8 Clause 6

- http://mykisscountry937.com/child-car-seat-alarm-systems-alert-you-when-child-is-left-in-hot-car/ (referred while making requirements)
- http://www.parents.com/baby/safety/car/danger-in-the-car/ (referred while making requirements)
- Why ATMEL is ok for 26262: http://www.atmel.com/Images/Atmel-4073-AVR-Microcontrollers-for-Automotive_Brochure.pdf
-