TATA ELXSI

Functional Safety in Automotive Grade Linux

Renjith G | Shilu S L

July 13, 2016, AGL Summit, Tokyo, Japan

Agenda

About Case Study

Roadmap – AGL

General - AGL

Functional Safety - AGL

Functional Safety Analysis - AGL

Audience, Takeaways

Areas / Intended Audience

✓Functional safety – ISO26262

✓IC,HUD use cases

✓Software Development - Automotive

✓GNU/Linux Subsystem

Takeaways

✓Basics of FS feasibility in AGL

✓Basics of FS process for AGL

✓FS specific Design strategies for IC & HUD SW

Consolidation

✓QnA

✓Further interests

Background / Key Motivation / Interest

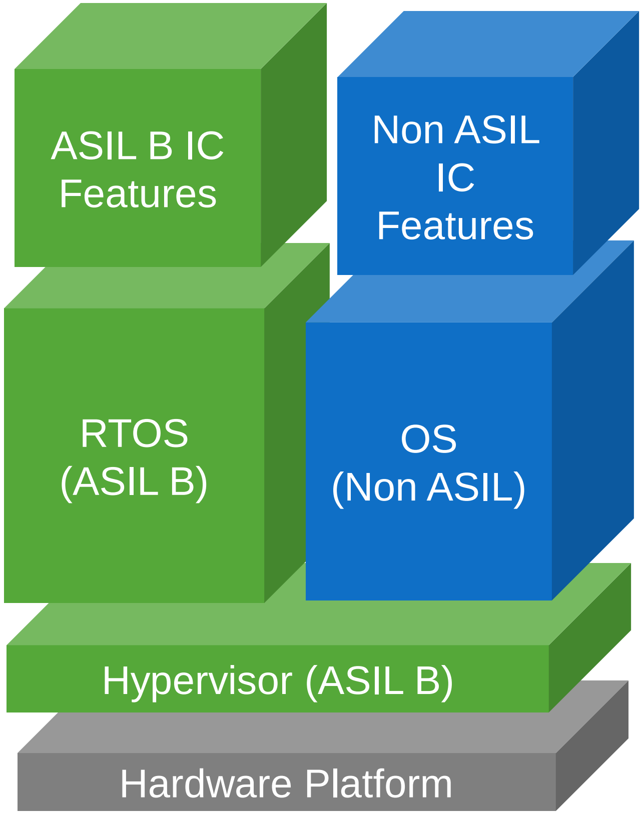
Quoting from [“https://www.automotivelinux.org/about”](https://www.automotivelinux.org/about)

“Automotive Grade Linux (AGL) is a Linux Foundation Workgroup dedicated to creating open source software solutions for automotive applications.
Although the initial target for AGL is In-Vehicle-Infotainment (IVI) systems, additional use cases such as ***“instrument clusters”*** *and telematics systems will eventually be supported.”*

Background / Key motivation/Interest

This case study checks the feasibility of implementing ***Instrument cluster + Head up display*** use cases in AGL where functional safety is a requirement.

Architecture Approaches – Safety Perspective


ASIL B IC Features

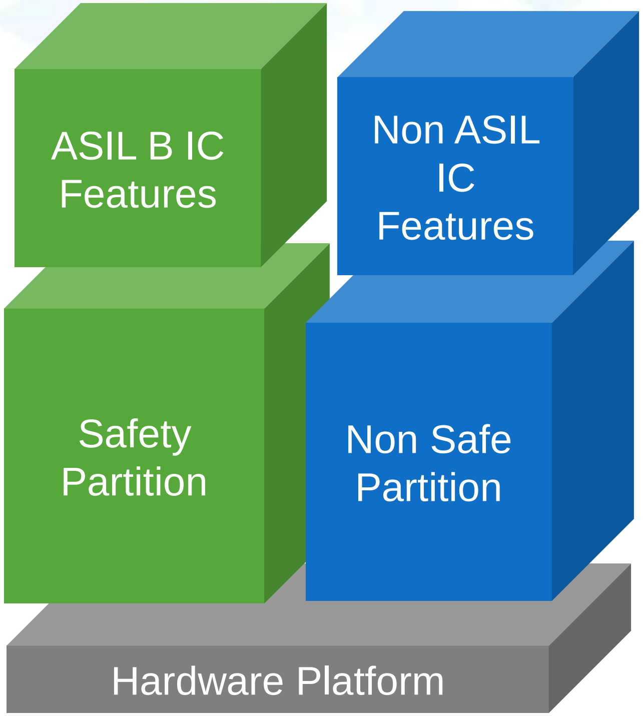
Non ASIL IC Features

RTOS (ASIL B)

OS (Non ASIL)

Hypervisor (ASIL B)

Hardware Platform


ASIL B IC Features

Non ASIL IC Features

Safety Partition

Non Safe Partition

Hardware Platform

Opensource ASIL B Hypervisors?
Opensource ASIL B RTOS?
Performance?
Complexity?
Cost?

Roadmap – in AGL

IC,HUD MW (ASIL B)

Fastboot in AGL

eCockpit in AGL

Functional safety in AGL

General – from AGL

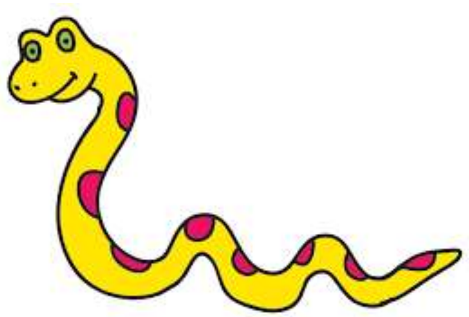
BSP and SOC	Renesas R-Car
Version	Agile Albacore
Kernel	3.10.31 LTSi

Functional Safety – Analysis in AGL

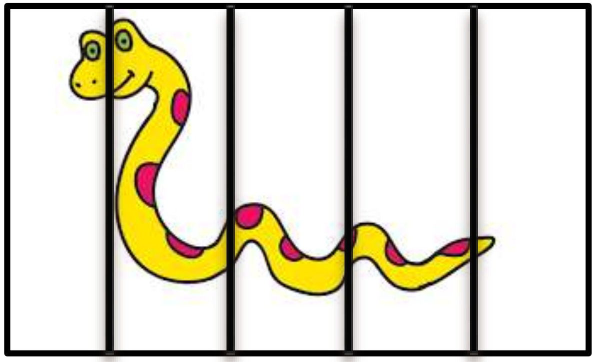
Functional Safety :

Absence of unacceptable **risk** due to **hazards** caused by malfunction behavior of systems

Risk = Exposure * Effect * Probability

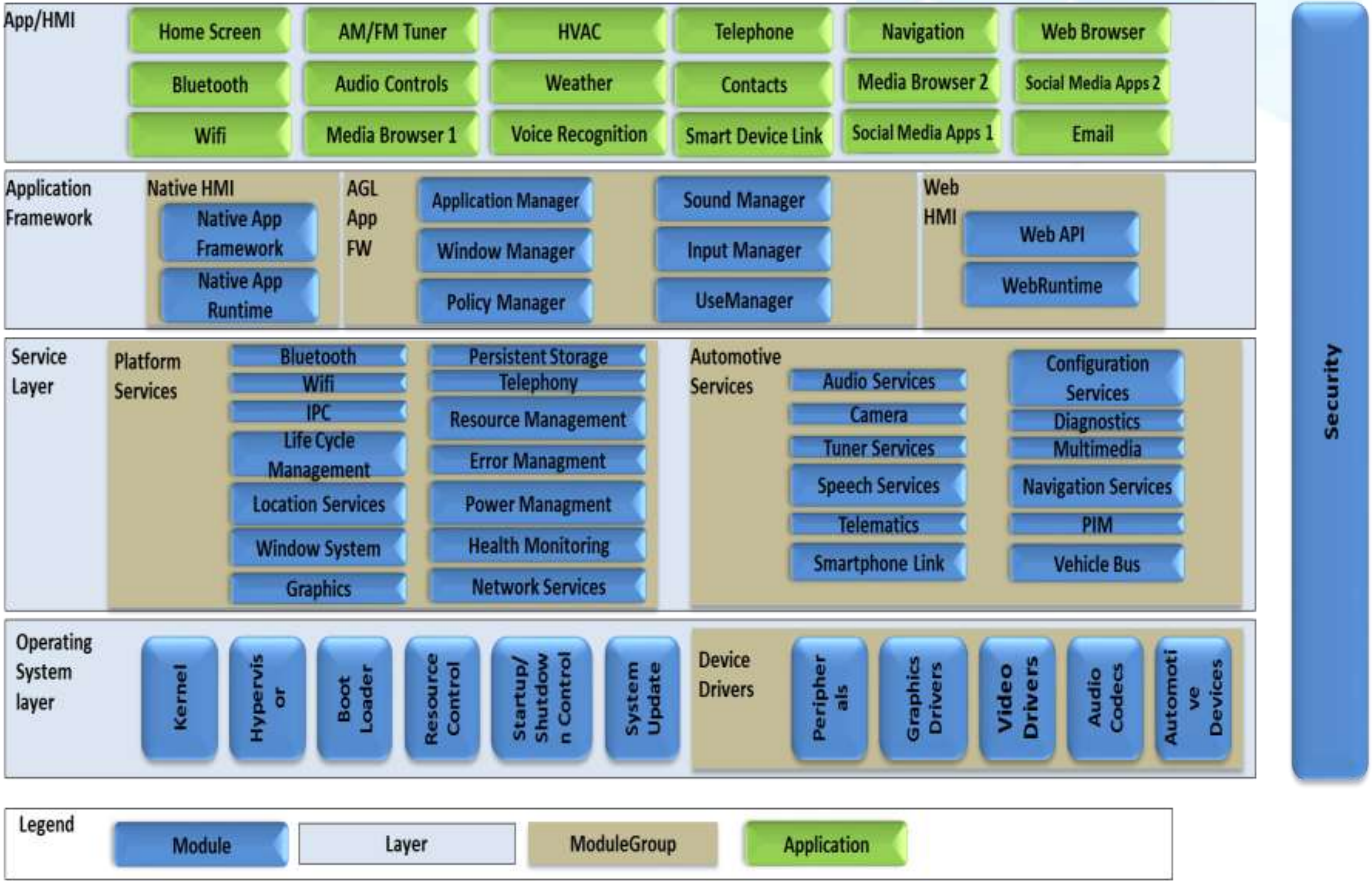


High Risk



Low Risk

Current Software Architecture - AGL



App/HMI

- Home Screen
- AM/FM Tuner
- HVAC
- Telephone
- Navigation
- Web Browser
- Bluetooth
- Audio Controls
- Weather
- Contacts
- Media Browser 2
- Social Media Apps 2
- Wifi
- Media Browser 1
- Voice Recognition
- Smart Device Link
- Social Media Apps 1
- Email

Application Framework

- Native HMI: Native App Framework, Native App Runtime
- AGL App FW: Application Manager, Window Manager, Policy Manager, Sound Manager, Input Manager, UseManager
- Web HMI: Web API, WebRuntime

Service Layer

- Platform Services: Bluetooth, Wifi, IPC, Life Cycle Management, Location Services, Window System, Graphics, Persistent Storage, Telephony, Resource Management, Error Managment, Power Managment, Health Monitoring, Network Services
- Automotive Services: Audio Services, Camera, Tuner Services, Speech Services, Telematics, Smartphone Link, Configuration Services, Diagnostics, Multimedia, Navigation Services, PIM, Vehicle Bus

Operating System layer

- Kernel
- Hypervisor
- Boot Loader
- Resource Control
- Startup/ Shutdown Control
- System Update
- Device Drivers: Peripherals, Graphics Drivers, Video Drivers, Audio Codecs, Automotive Devices

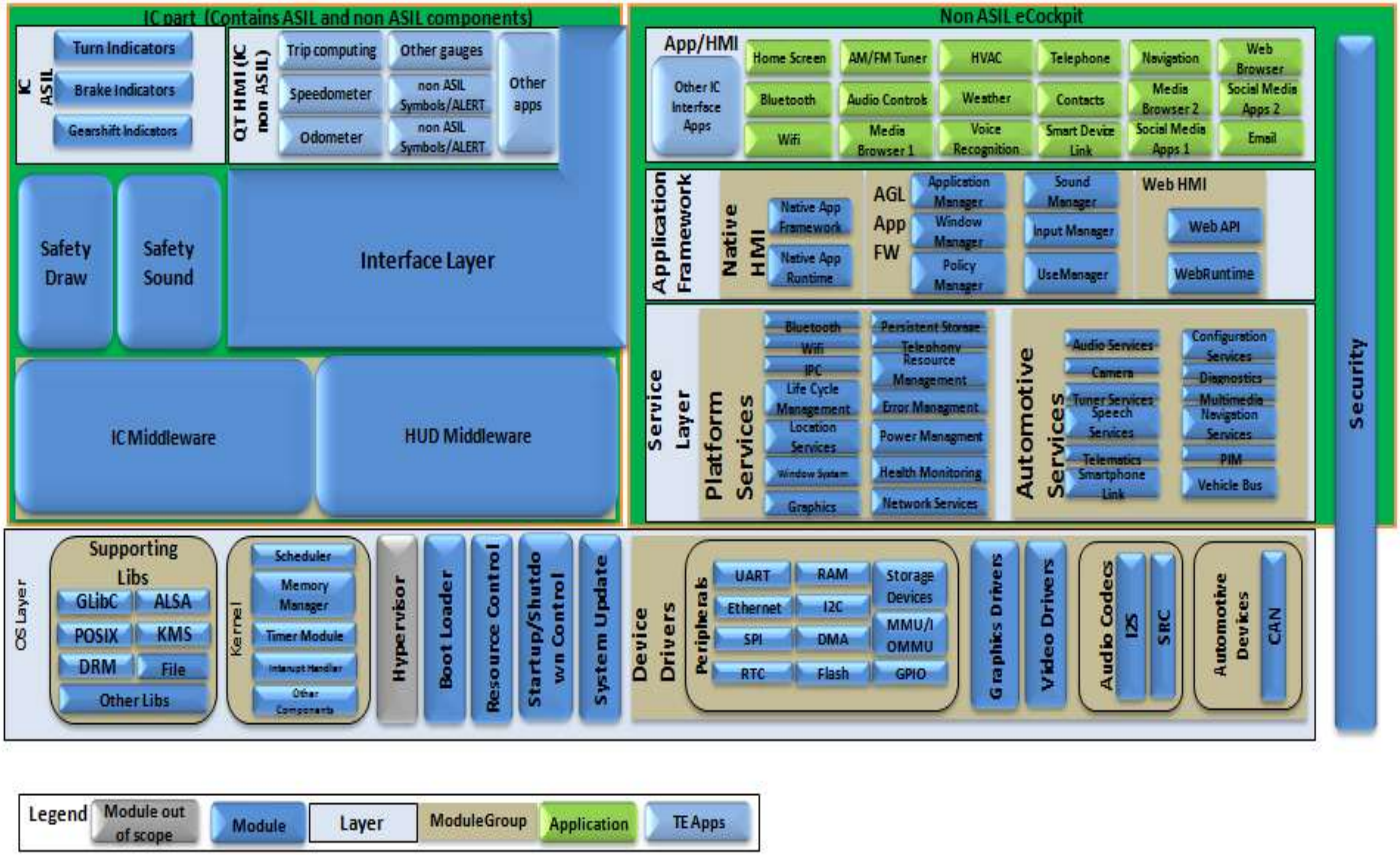
Security

Legend

- Module
- Layer
- ModuleGroup
- Application

Source: AGL Specification 1.0

Derived - Software Architecture with Safety Stack – in AGL



IC part (Contains ASIL and non ASIL components)

IC ASIL
Turn Indicators
Brake Indicators
Gearshift Indicators

QT HMI (IC non ASIL)
Trip computing
Other gauges
Speedometer
non ASIL Symbols/ALERT
Odometer
non ASIL Symbols/ALERT
Other apps

Safety Draw
Safety Sound
Interface Layer
IC Middleware
HUD Middleware

Non ASIL eCockpit

App/HMI
Other IC Interface Apps
Home Screen
AM/FM Tuner
HVAC
Telephone
Navigation
Web Browser
Bluetooth
Audio Controls
Weather
Contacts
Media Browser 2
Social Media Apps 2
Wifi
Media Browser 1
Voice Recognition
Smart Device Link
Social Media Apps 1
Email

Application Framework
Native HMI
Native App Framework
Native App Runtime
AGL App FW
Application Manager
Window Manager
Policy Manager
Sound Manager
Input Manager
UseManager
Web HMI
Web API
WebRuntime

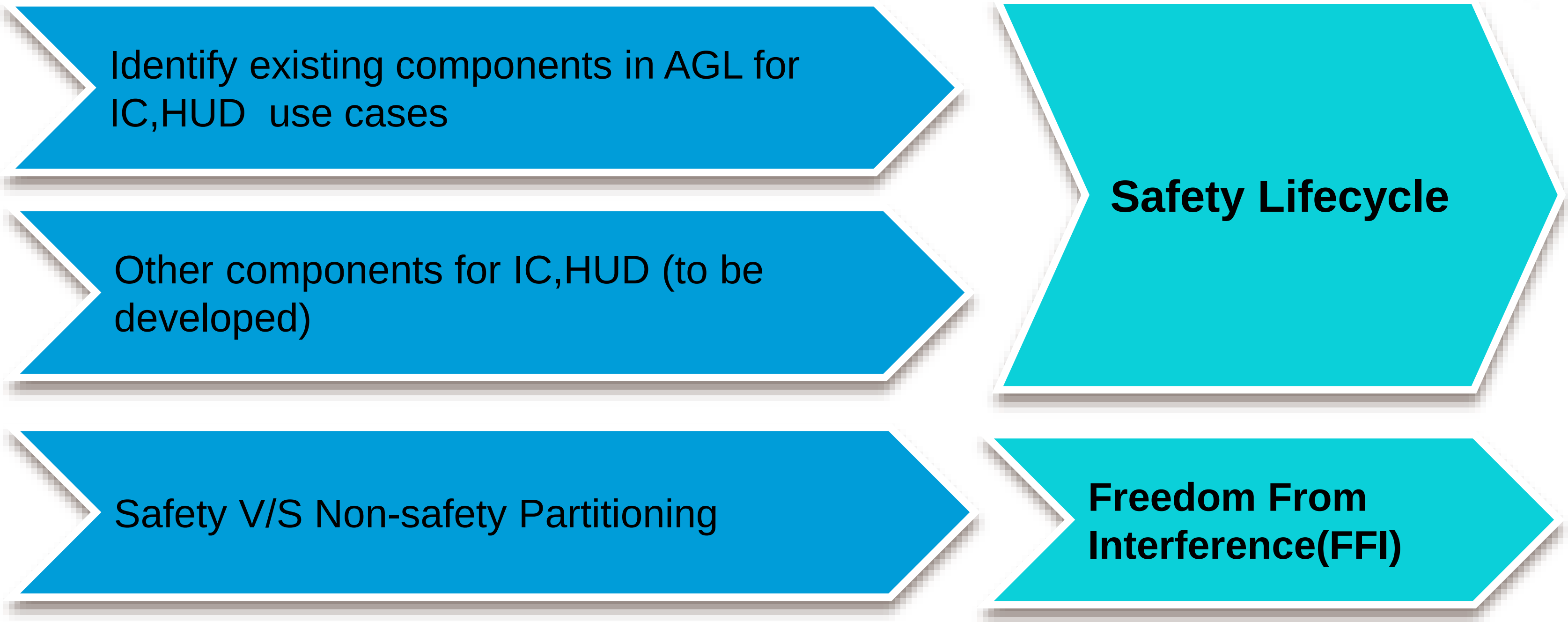
Service Layer
Platform Services
Bluetooth
Wifi
IPC
Life Cycle Management
Location Services
Window System
Graphics
Persistent Storage
Telephony
Resource Management
Error Managment
Power Managment
Health Monitoring
Network Services
Automotive Services
Audio Services
Camera
Tuner Services
Speech Services
Telematics
Smartphone Link
Configuration Services
Diagnostics
Multimedia
Navigation Services
PIM
Vehicle Bus

Security

OS Layer
Supporting Libs
GLibC
ALSA
POSIX
KMS
DRM
File
Other Libs
Kernel
Scheduler
Memory Manager
Timer Module
Interupt Handler
Other Components
Hypervisor
Boot Loader
Resource Control
Startup/Shutdown Control
System Update
Device Drivers
Peripherals
UART
RAM
Storage Devices
Ethernet
I2C
MMU/IOMMU
SPI
DMA
RTC
Flash
GPIO
Graphics Drivers
Video Drivers
Audio Codecs
I2S
SRC
Automotive Devices
CAN

Legend
Module out of scope
Module
Layer
ModuleGroup
Application
TE Apps

Way To Functional Safety Compliance – in AGL Arch



Identify existing components in AGL for IC,HUD use cases

Other components for IC,HUD (to be developed)

Safety V/S Non-safety Partitioning

Safety Lifecycle

Freedom From Interference(FFI)

ISO 26262

Existing components and Tools used – in AGL

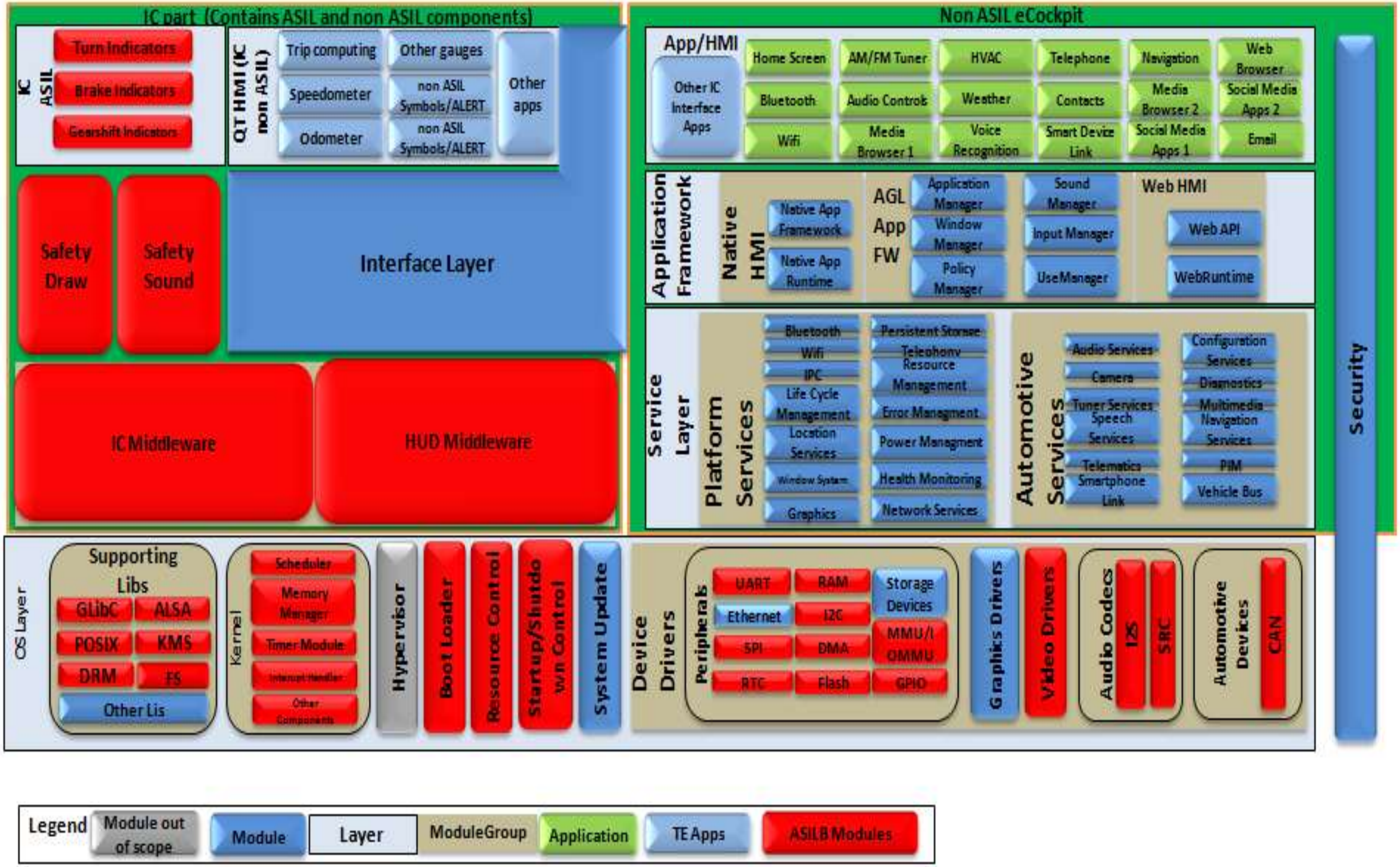
- Kernel (v3.10)
  - Task management
  - Memory Management
  - Protection
- Device Drivers
- Libraries
  - GLIBC (v2.20)
  - POSIX
  - ALSA (v1.0.28)
  - DRM (v2.4)
  - KMS (v1.4.0)

- Other Tools used
  - gcc for arm Compiler (v4.9.1)
  - DOORS/Microsoft Office Excel for SRS.
  - Enterprise Architect 12.0 for SAD
  - Enterprise Architect 12.0 for SUD
  - Source code editor (Vim)
  - Static analyzing tool (QAC 8.1)
  - Unit testing tool(TESSY 2.3)
  - Version control tool (SVN)

Other components for IC,HUD use cases – in AGL

- ❑ Instrument Cluster Middleware
- ❑ HUD Middleware
- ❑ Interface Layer
- ❑ Safety draw
- ❑ Safety sound
- ❑ Safety critical applications
- ❑ ASIL Compliant HMI Tool (Third party – Option 2)

Derived - Software Architecture with Safety Stack – in AGL ASIL B Highlighted – Option 1



IC part (Contains ASIL and non ASIL components)

IC ASIL
Turn Indicators
Brake Indicators
Gearshift Indicators

QT HMI (IC non ASIL)
Trip computing
Other gauges
Speedometer
non ASIL Symbols/ALERT
Odometer
non ASIL Symbols/ALERT
Other apps

Safety Draw
Safety Sound
Interface Layer
IC Middleware
HUD Middleware

Non ASIL eCockpit

App/HMI
Other IC Interface Apps
Home Screen
AM/FM Tuner
HVAC
Telephone
Navigation
Web Browser
Bluetooth
Audio Controls
Weather
Contacts
Media Browser 2
Social Media Apps 2
Wifi
Media Browser 1
Voice Recognition
Smart Device Link
Social Media Apps 1
Email

Application Framework
Native HMI
Native App Framework
Native App Runtime
AGL App FW
Application Manager
Window Manager
Policy Manager
Sound Manager
Input Manager
UseManager
Web HMI
Web API
WebRuntime

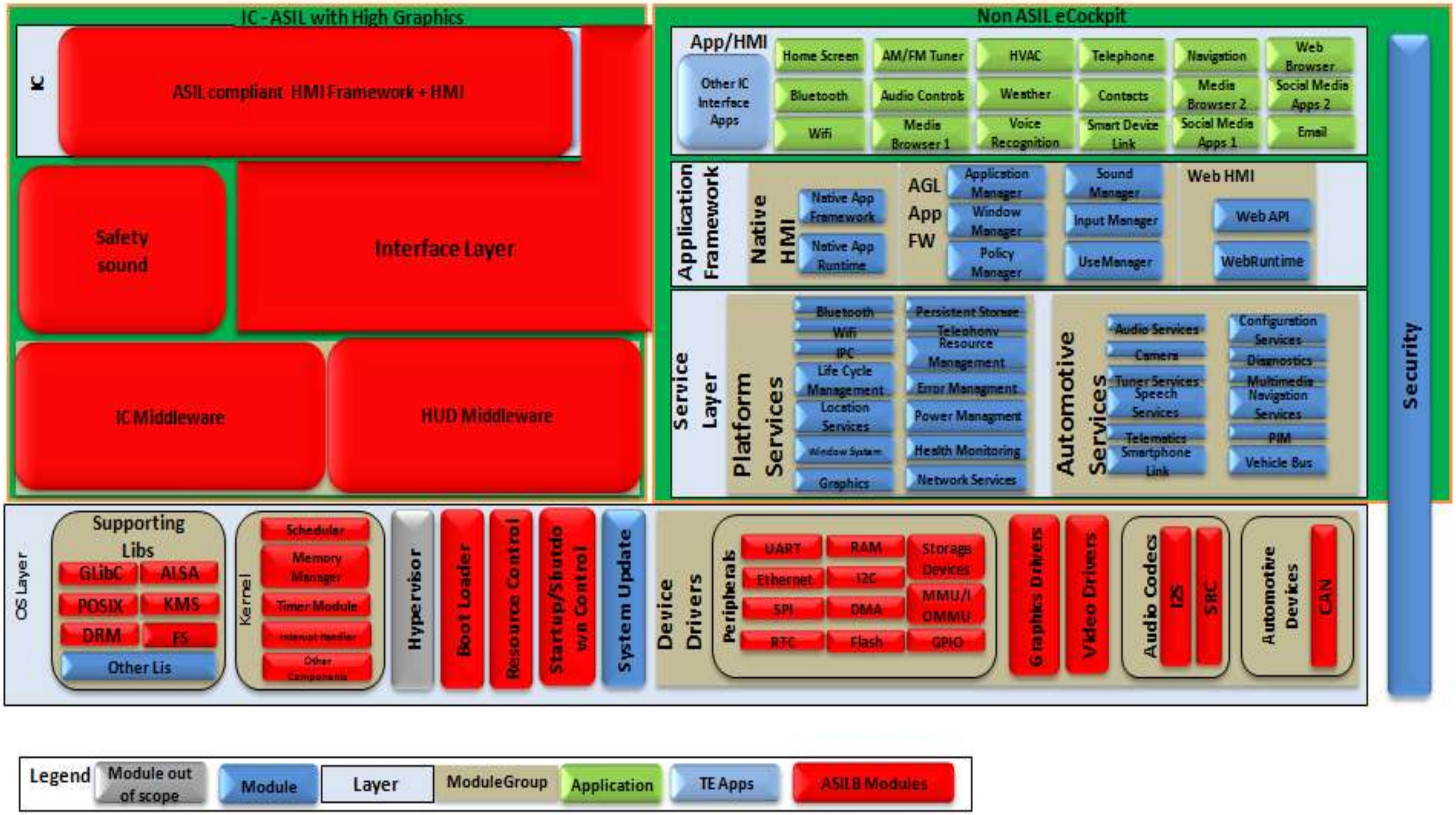
Service Layer
Platform Services
Bluetooth
Wifi
IPC
Life Cycle Management
Location Services
Window System
Graphics
Persistent Storage
Telephony
Resource Management
Error Managment
Power Managment
Health Monitoring
Network Services
Automotive Services
Audio Services
Camera
Tuner Services
Speech Services
Telematics
Smartphone Link
Configuration Services
Diagnostics
Multimedia
Navigation Services
PIM
Vehicle Bus

Security

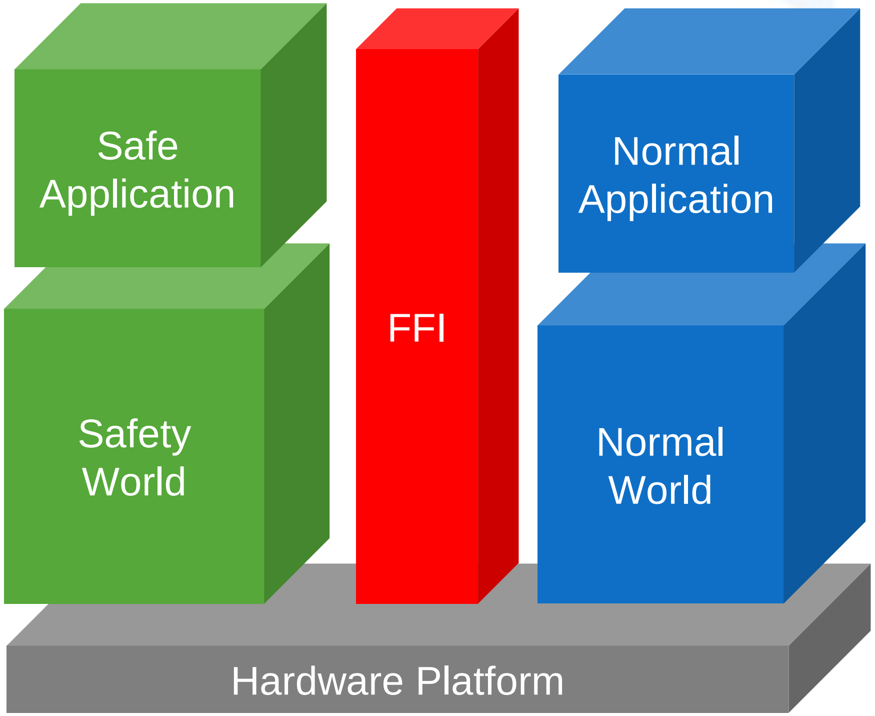
OS Layer
Supporting Libs
GLibC
ALSA
POSIX
KMS
DRM
FS
Other Lis
Kernel
Scheduler
Memory Manager
Timer Module
Interrupt Handler
Other Components
Hypervisor
Boot Loader
Resource Control
Startup/Shutdown Control
System Update
Device Drivers
Peripherals
UART
RAM
Storage Devices
Ethernet
I2C
MMU/IOMMU
SPI
DMA
RTC
Flash
GPIO
Graphics Drivers
Video Drivers
Audio Codecs
I2S
SRC
Automotive Devices
CAN

Legend
Module out of scope
Module
Layer
ModuleGroup
Application
TE Apps
ASILB Modules

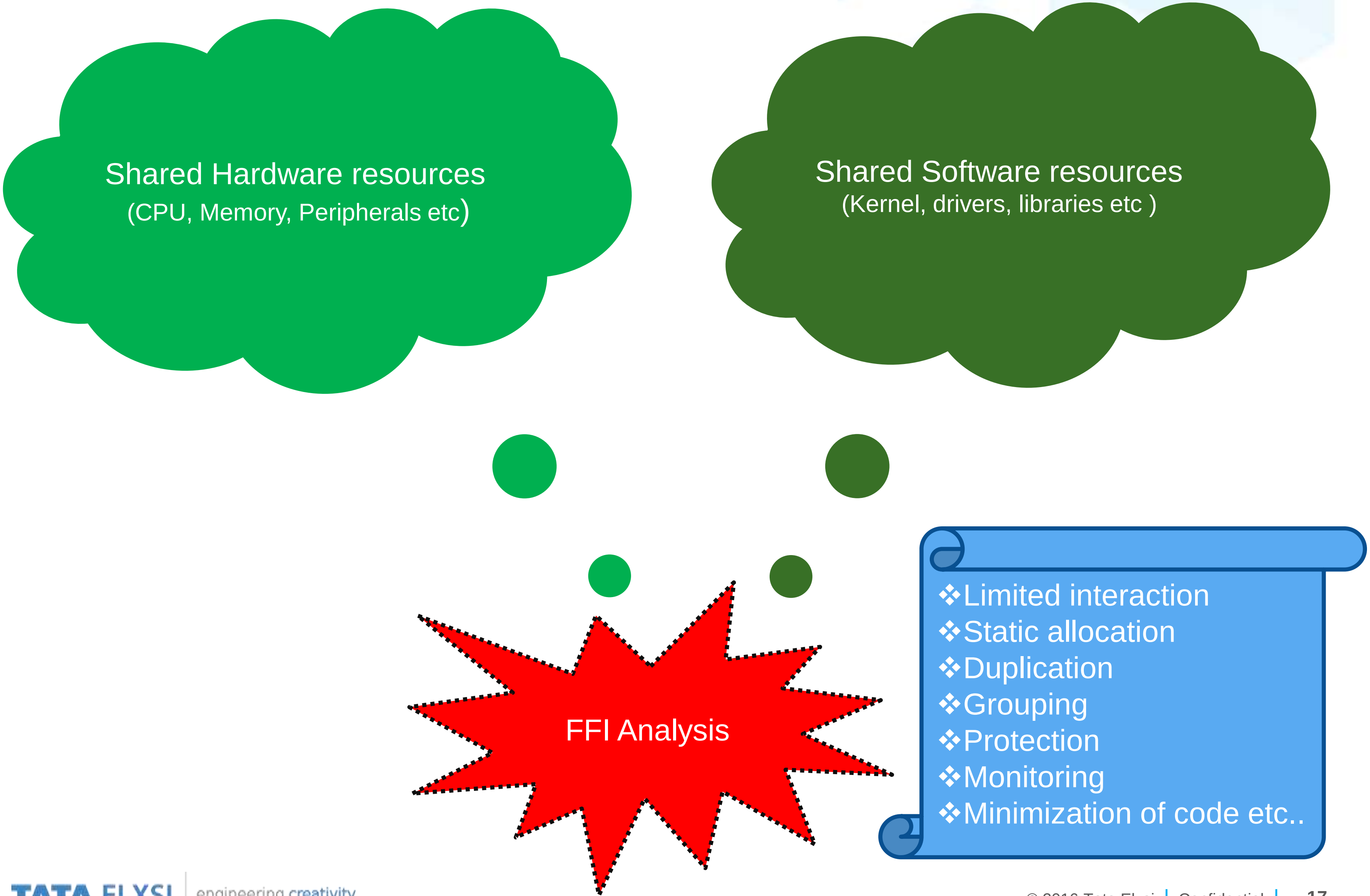
Derived - Software Architecture with Safety Stack – in AGL ASIL B Highlighted – Option 2



Safety Software Architecture(Partitioning) – in AGL



Safety Software Architecture – Freedom From Interference



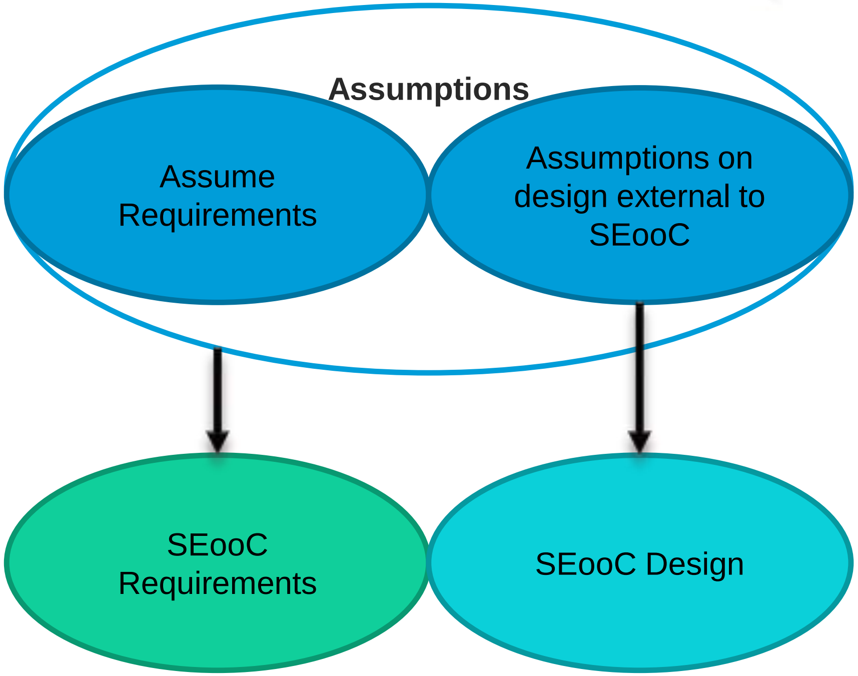
Shared Hardware resources
(CPU, Memory, Peripherals etc)

Shared Software resources
(Kernel, drivers, libraries etc)

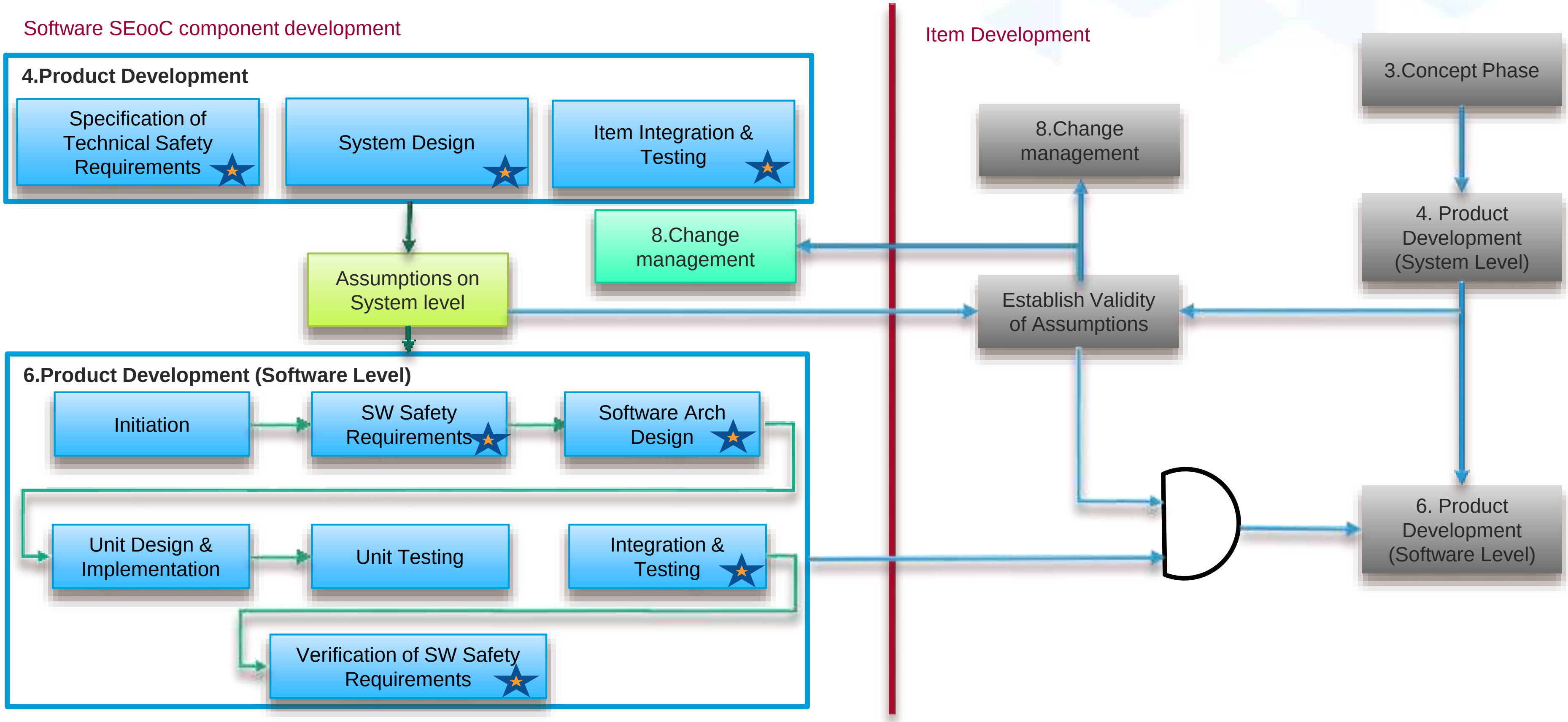
FFI Analysis

- ❖Limited interaction
- ❖Static allocation
- ❖Duplication
- ❖Grouping
- ❖Protection
- ❖Monitoring
- ❖Minimization of code etc..

Safety Lifecycle - SEooC – Safety Element Out Of Context



SEooC – S/W Development

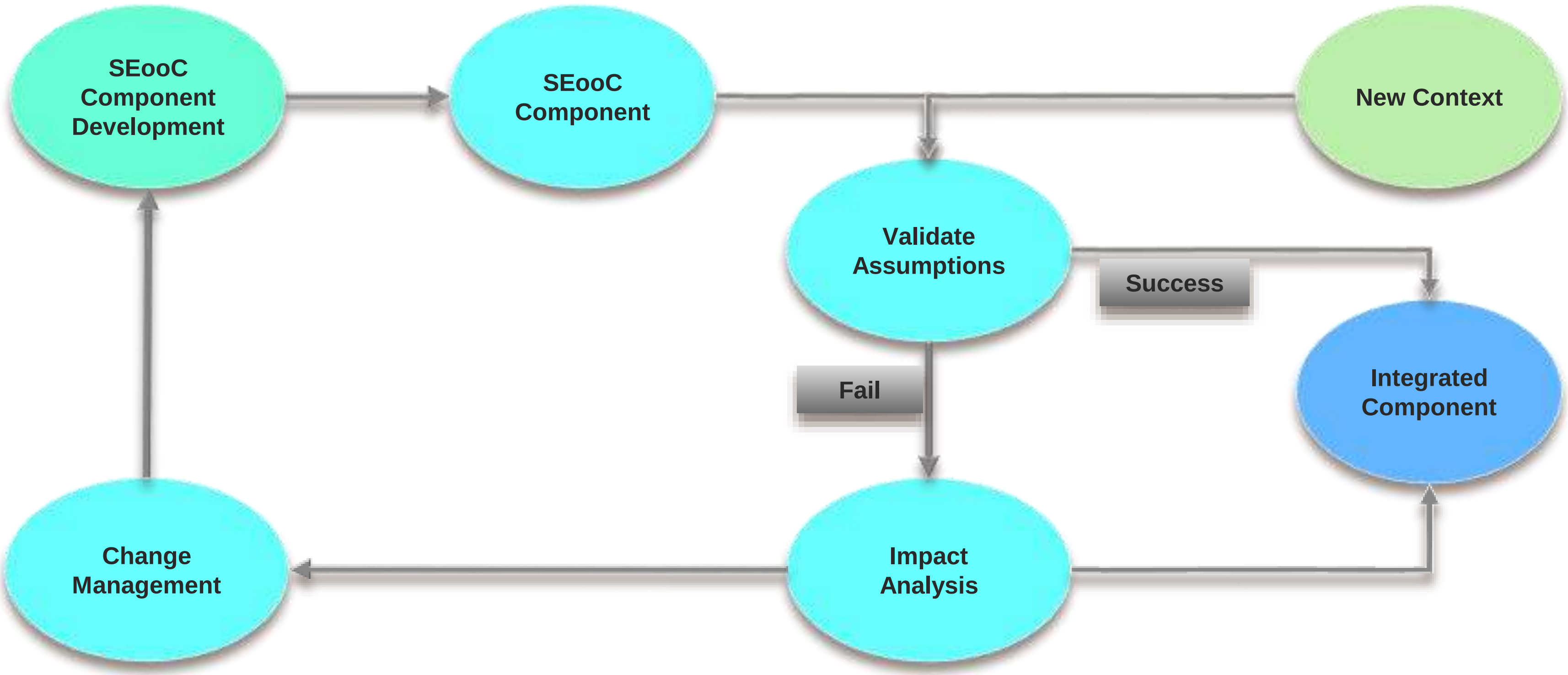


Software SEooC component development

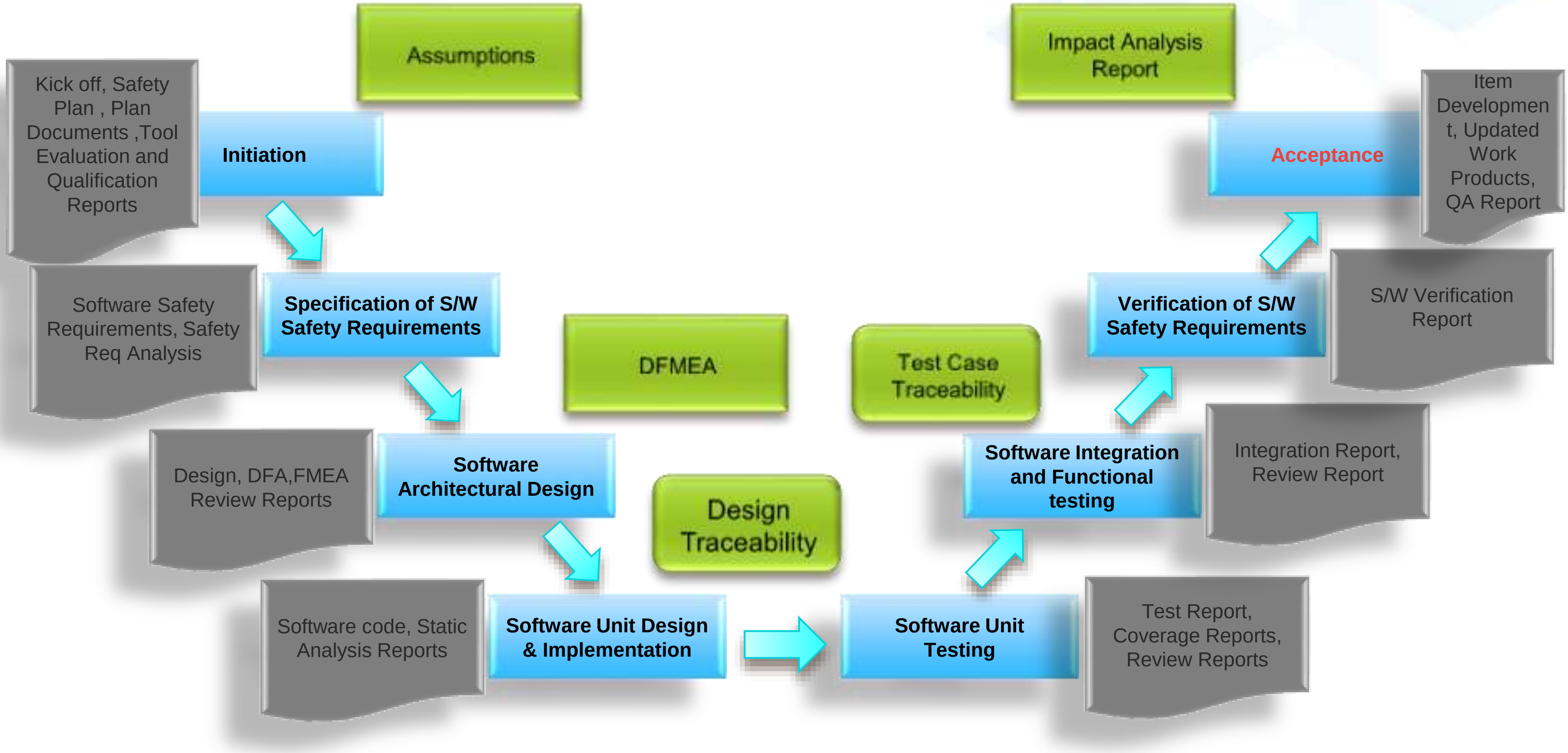
Item Development

4.Product Development
Specification of Technical Safety Requirements
System Design
Item Integration & Testing
8.Change management
Assumptions on System level
6.Product Development (Software Level)
Initiation
SW Safety Requirements
Software Arch Design
Unit Design & Implementation
Unit Testing
Integration & Testing
Verification of SW Safety Requirements
3.Concept Phase
8.Change management
4. Product Development (System Level)
Establish Validity of Assumptions
6. Product Development (Software Level)

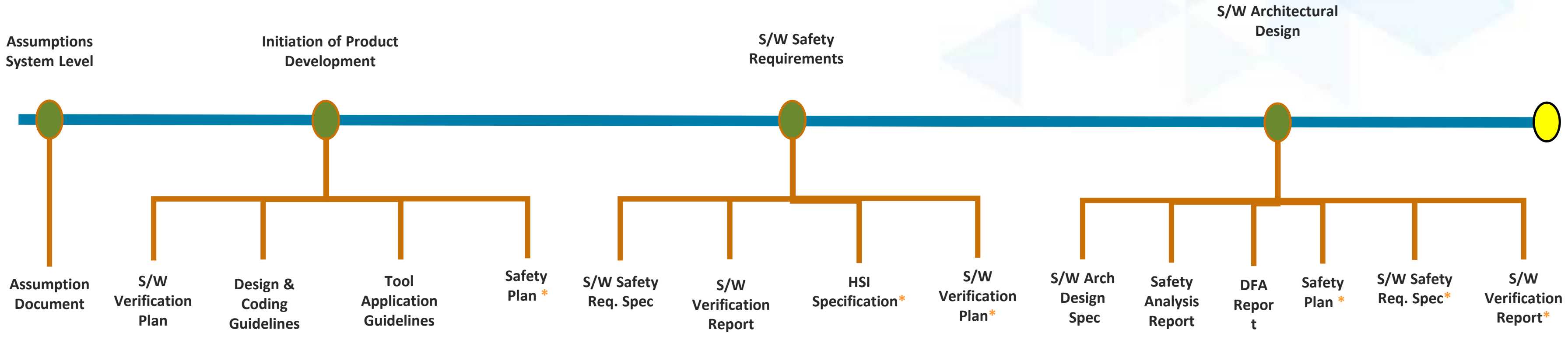
SEooC - Component Integration



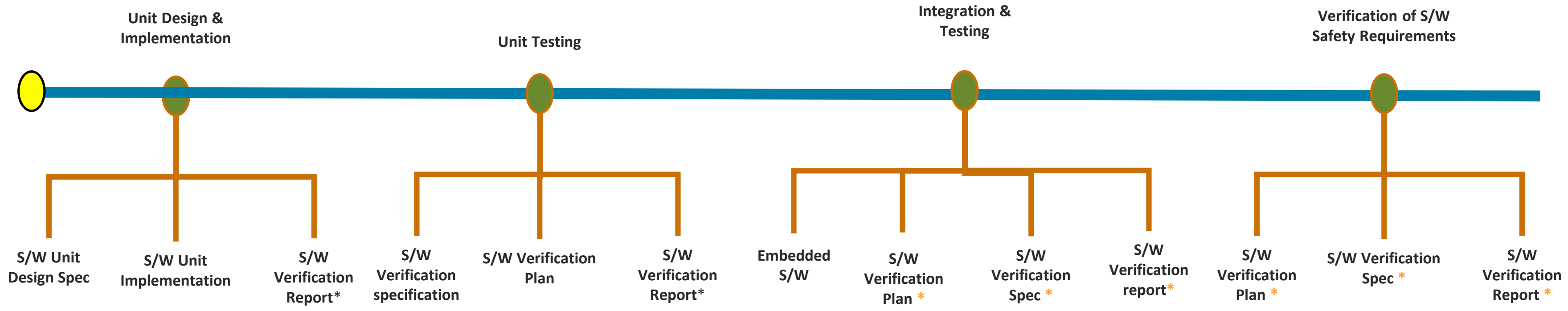
SEooC – The Process (V Model)


Assumptions
Impact Analysis Report
Kick off, Safety Plan , Plan Documents ,Tool Evaluation and Qualification Reports
Initiation
Acceptance
Item Development, Updated Work Products, QA Report
Software Safety Requirements, Safety Req Analysis
Specification of S/W Safety Requirements
DFMEA
Test Case Traceability
Verification of S/W Safety Requirements
S/W Verification Report
Design, DFA,FMEA Review Reports
Software Architectural Design
Design Traceability
Software Integration and Functional testing
Integration Report, Review Report
Software code, Static Analysis Reports
Software Unit Design & Implementation
Software Unit Testing
Test Report, Coverage Reports, Review Reports

SEooC - PART-6 OutComes



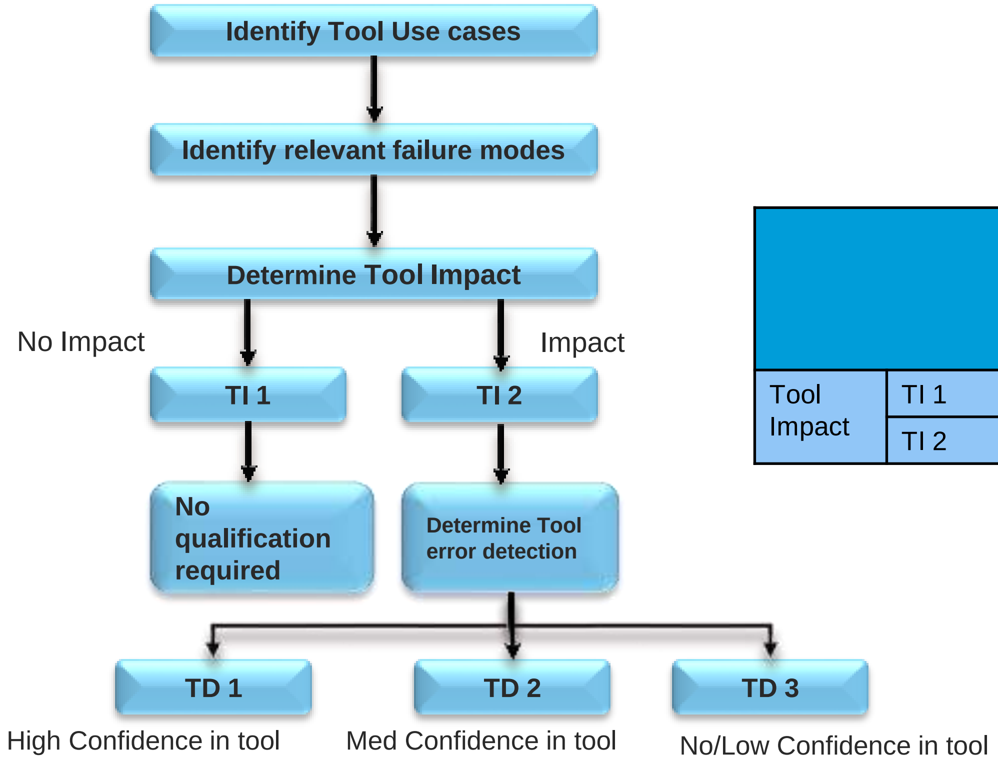
- Assumptions System Level
  - Assumption Document
- Initiation of Product Development
  - S/W Verification Plan
  - Design & Coding Guidelines
  - Tool Application Guidelines
  - Safety Plan *
- S/W Safety Requirements
  - S/W Safety Req. Spec
  - S/W Verification Report
  - HSI Specification*
  - S/W Verification Plan*
- S/W Architectural Design
  - S/W Arch Design Spec
  - Safety Analysis Report
  - DFA Repor t
  - Safety Plan *
  - S/W Safety Req. Spec*
  - S/W Verification Report*



- Unit Design & Implementation
  - S/W Unit Design Spec
  - S/W Unit Implementation
  - S/W Verification Report*
- Unit Testing
  - S/W Verification specification
  - S/W Verification Plan
  - S/W Verification Report*
- Integration & Testing
  - Embedded S/W
  - S/W Verification Plan *
  - S/W Verification Spec *
  - S/W Verification report*
- Verification of S/W Safety Requirements
  - S/W Verification Plan *
  - S/W Verification Spec *
  - S/W Verification Report *

NOTE: For detailed information about process, Refer ISO26262 Part6

SEooC – Tool Classification

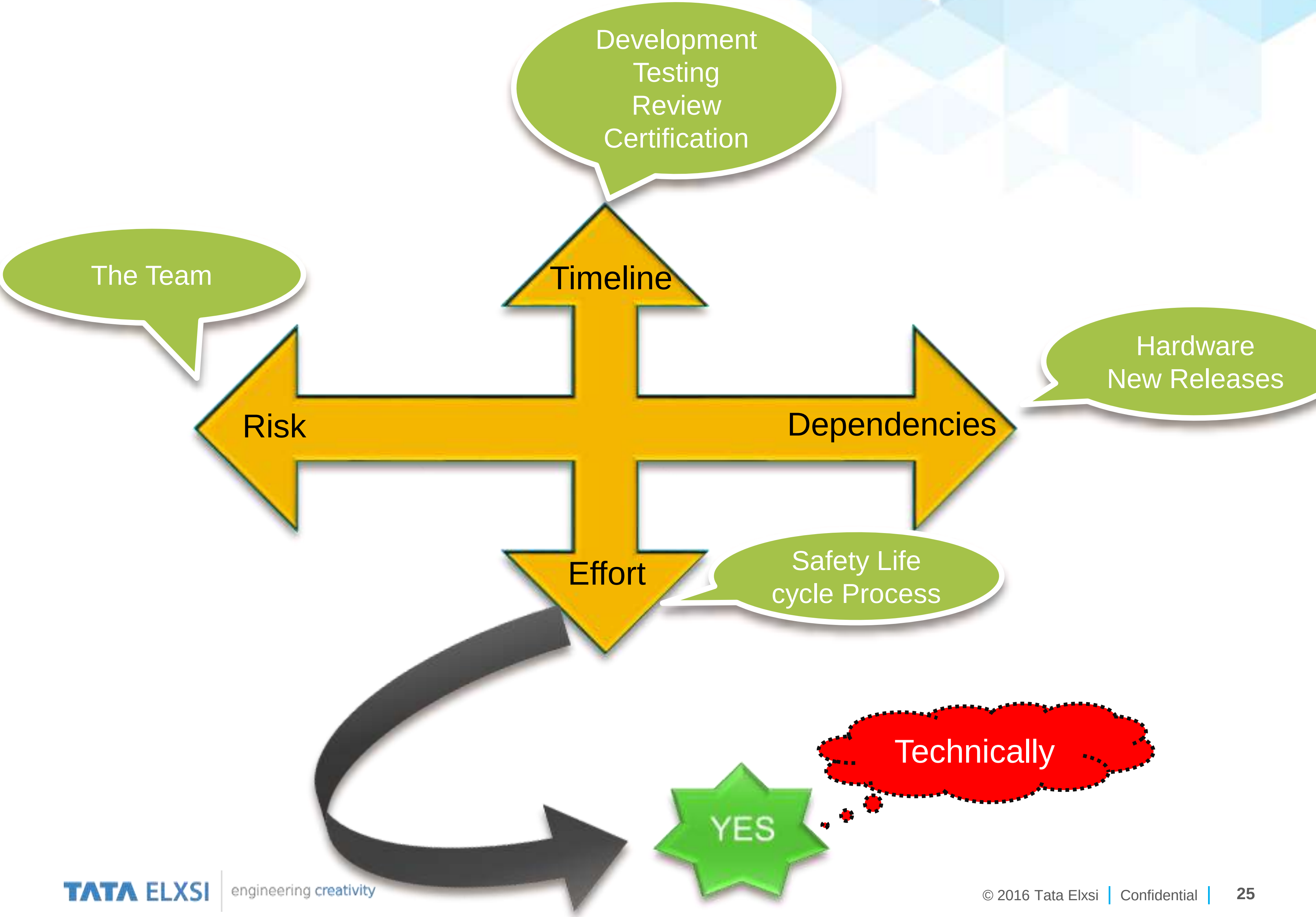


		Tool Error Detection		
		TD1	TD2	TD3
Tool Impact	TI 1	TCL 1	TCL 1	TCL 1
	TI 2	TCL 1	TCL 2	TCL 3

SEooC – Tool Qualification

Method	TCL 1	TCL 2				TCL 3			
		ASIL				ASIL			
		A	B	C	D	A	B	C	D
Increased confidence from use	No Qualification method Required	++	++	++	+	++	++	+	+
Evaluation of the development process		++	++	++	+	++	++	+	+
Validation of the software tool		+	+	+	++	+	+	++	++
Development in compliance with a safety standard		+	+	+	++	+	+	++	++

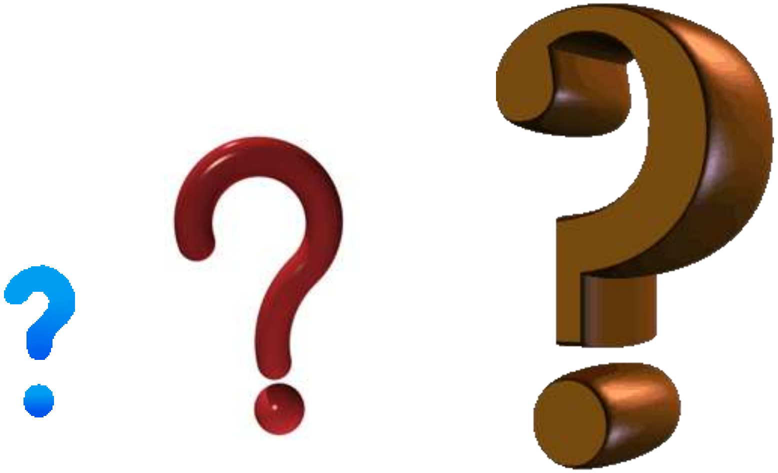
Conclusion - Feasibility



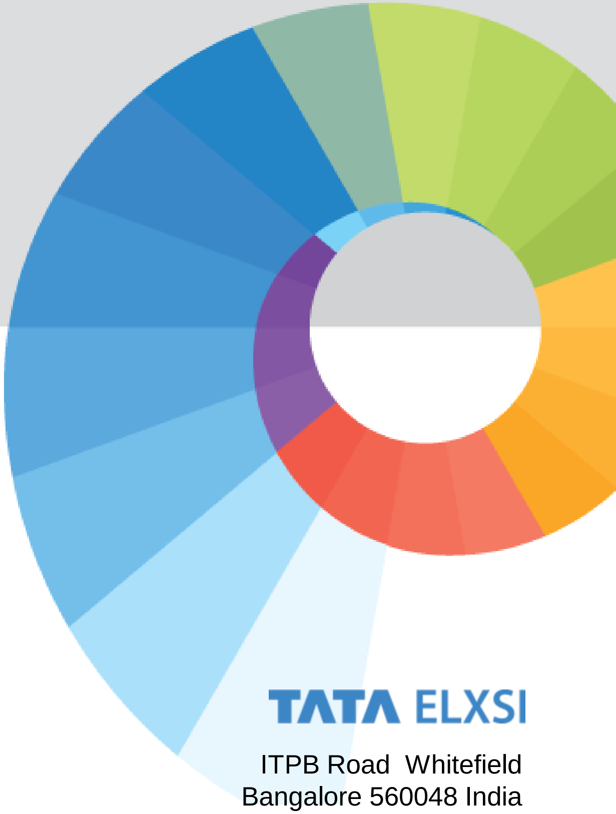
References

1. *https://www.automotivelinux.org*
2. *http://man7.org/linux/man-pages/*
3. *ISO26262:2011 Standard*

Questions and Answers



Thank You



Renjith G | Shilu SL

renjithg@tataelxsi.co.in | shilu@tataelxsi.co.in

+91 471 666 1138 | +91 471 666 1333

TATA ELXSI

ITPB Road Whitefield
Bangalore 560048 India
Tel +91 80 2297 9123 | Fax +91 80 2841 1474
e-mail info@tataelxsi.com

www.tataelxsi.com