27/11/2019

Failures — Omission - Intended Funxn failure
E.g.: Brakes not working, with vehicle in front.
Commission - Wrong decisions / predictions.
E.g.: High risks at higher speeds with vehicle in-rear (Applied when not required).

FMEA :- is a systemised group of activities intended to:-
(a) recognize and evaluate the potential failure of product and its effects,
(b) identify actions (e.g.: Safety mech.) which prevents or reduce the chance of pot. failure, and
(c) Document the process. Update design/process accordingly.

① Def^n: method to identify the all possible potential failures in design/process, evaluate them in terms of Severity, Occurence and Detection ~~which that~~ and address ways to mitigate the potential failures.

② Def^n: analytical technique to identify all possible pot. failur in design, evaluate them in terms of Sev, Occ and detec^n, and address ways to mitigate identified potential failures.

① why ISO 26262 required?
→ With increase of advanced systems in automotive industry, the no. of ECUs used and associated complexity increases. This results in increased efforts to create safety-compliant systems.

In order to manage the complexity and to master functional safety aspects, we need a structured guideline which specifies all aspects of development lifecycle. Hence, ISO 26262 is required.

For. e.g:- Brake-by-wire → In this, the ECU must always be informed about driver's intentions to brake or to stop the vehicle. Therefore, missing the "pedal sensor" data is a serious problem for functionality of Veh. ctrl. sys. which would ~~be~~ endanger human lives.
~~Also~~ Also "wheel speed sensor" data in Brake-by-wire helps to avoid skidding. Missing some of data samples from safety-critical sensors shall be safeguarded during designing. Soln can be redundant sensors or a fail-safe mechanism. Also ECU can suffer from intermittent (temporary) data loss, due to problem with sensor or with data transmission path / short circuit / discanxn / communic^n

29/11/19

(2) What are the steps followed in performing Design failure mode and effect analysis?

→ Obj: To detect errors in early design phases.

Step 1:

(a) Identify all functions within scope
- list measurable functions and Potential Failure Modes leading to the loss/reduction of each function.

E.g.: Support transmission, stop vehicle
(x kgs per specfc xyz) (x feet from Yspect to meet xyz)

(b) Identify how each function can fail (Failure Modes)
- Pot. Failure Mode — is the manner in which a component / subsystem / system could potentially fail to meet / deliver intended function
- Pot. Failure Mode may also be the cause of a potential failure mode.
- Pot. failure Mode types
  - (i) No Function
  - (ii) Partial / Over Function / Degraded Over Func.
    - meets some req, but does not fully comply
  - (iii) Intermittent function.
  - (iv) Unintended function
    - includes failures caused by s/m interaction.

E.g.: (a) Unrequested operation.
(b) Operation in an unintended direction
(c) Inadvertent operation

(c) Potential Effects of failure
* Can effect safety or regulations
E.g.: Noise, degraded function, intermitt-ent operation.

(d) Severity — seriousness of effect

Step 2:

(e) Potential causes of failure
Assuming * Item is manufactured within engineering specifications and/or * Design may include a deficiency that may cause unacceptable varia" (E.g., misbuilds, errors) in manufacturing.
E.g.: Torque specified too low, item upside down :: Symmetrical design.

(f) Estimate Occurence

(g) Classification — critical (sev = 9 or 10)
— significant (sev = 5 to 8)

Note:-
System
└ chassis, power train, Interior s/m

Sub-System
└ Front suspension of chassis s/m

Component
└ strut of front suspension

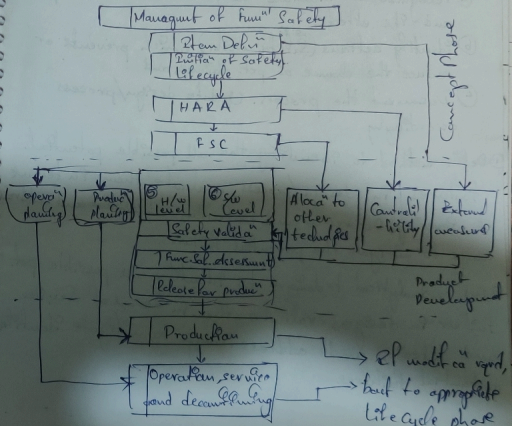
MOVICOL LIQUID

*Deductive - (Top Down) and Inductive (Bottom-up)

- systematically identifying causes of undesirable effect
- predicting effects of a prior events known problems such as faults.

E.g: Fault Tree Analysis
Effects known → Find → Effects Causes

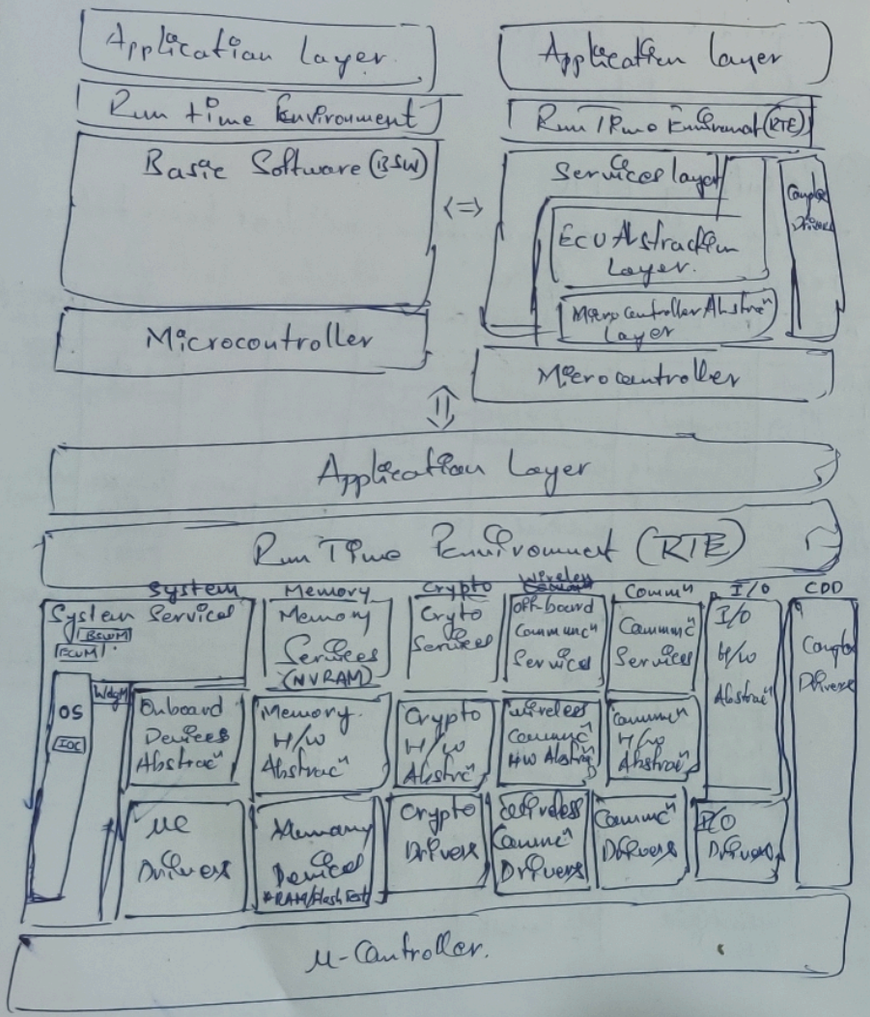
E.g: Failure Mode and Eff. Analysis.
Effects known ← Find ← Causes



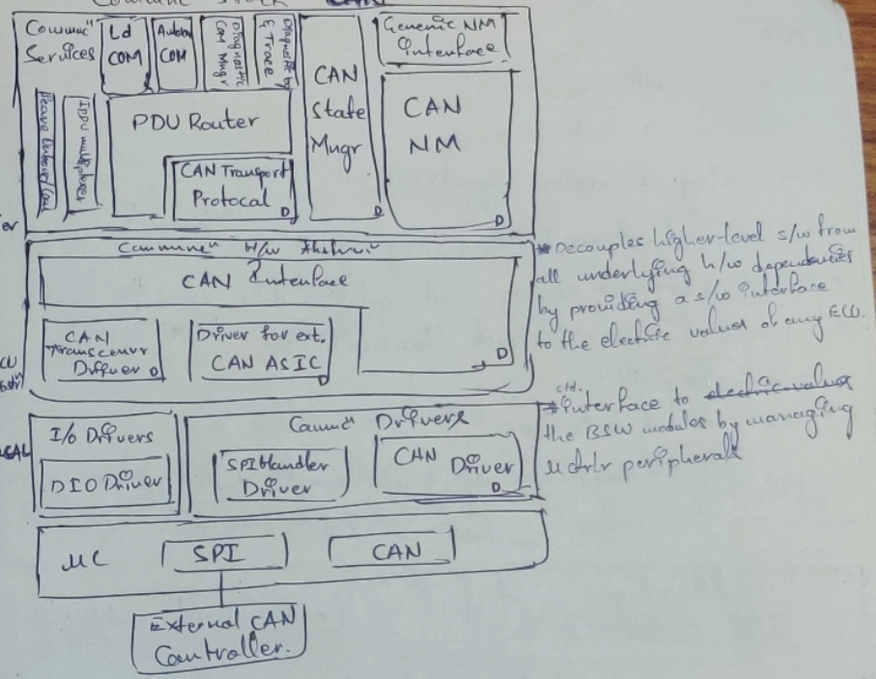
MOVICOL

MOVICOL LIQUID

11/12/2019



Communication Stack – CAN

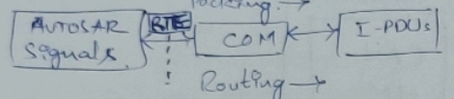


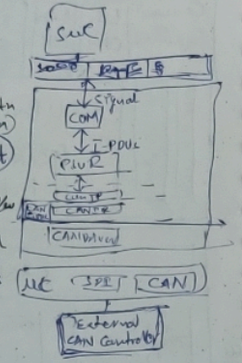
* Decouples higher-level s/w from all underlying h/w dependencies by providing a s/w interface to the electric values of any ECU.

* Interface to std. the BSW modules by managing µ ctrlr peripherals

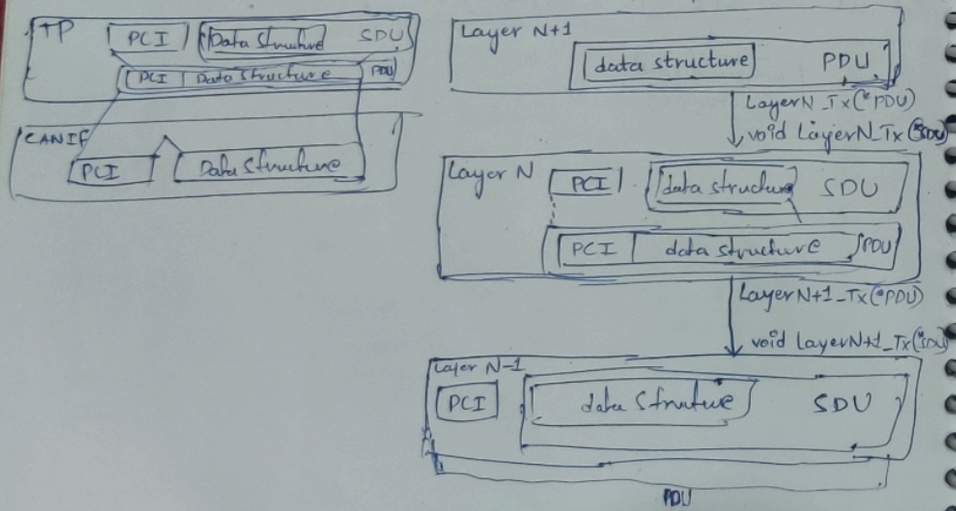
13/12/19

COM:





* Monitoring of receive signals (Signals Timeout)
* Filter mechanism for incoming signals
* Provision of init values and update indications
* Support of two different transmission modes per I-PDU
* Signal based gateway
* Support of large and dynamic length data types
  → I-PDU counters and I-PDU replica.



PDU:

PDUs composed of protocol specific control information and user data.

In layered architectures of communication protocol stacks, each layer implements protocols tailored to the specific type/mode of data exchange.

OSI layer	PDU
1 Physical Layer	Bit/Symbol
2 Data link layer	Frame
3 Network layer	Packet
4 Transport layer	Segment or Datagram

Physical layer - Sending ones and zeros across a wire, fiber, etc.

Data link layer - Organizing the ones and zeros ~~across a wire~~ into chunks of data and getting them safely to the right place on the wire.

Network layer - Passing data chunks over multiple connected networks.

Transport layer - Delivery of the data to the right s/w application at the destination is done by Transport layer.

Internet Protocol Suite

Transport Layer	TCP - Segment UDP - Datagram
Internet layer	Packet
Link Layer	Frame

Step 3 :- 6/12/19

(h) Current prevention controls used to establish occurence → Reduce the rate of occurence.

~~(i) Current detection control~~

- Design controls includes design reviews, analytical studies and computer model program tests equivalent to design verification tests.

(i) current detection control.

- validation and/or verification activities has to be improved.

(j) Detection Rating (0 to 10)

(k) Initial RPN

(l) Recommended Actions (Prevention and Detection)

- Severity Ranking - reduced only through design revision.

- Then Occurence Rating - ~~red~~ can be affected only by removing or controlling ~~one~~/more of the causes/Mechanisms of the failure Mode through a design revision.

E.g.:- perform comp. simulation to assure functioning in required temp. range.

(m) Actions taken

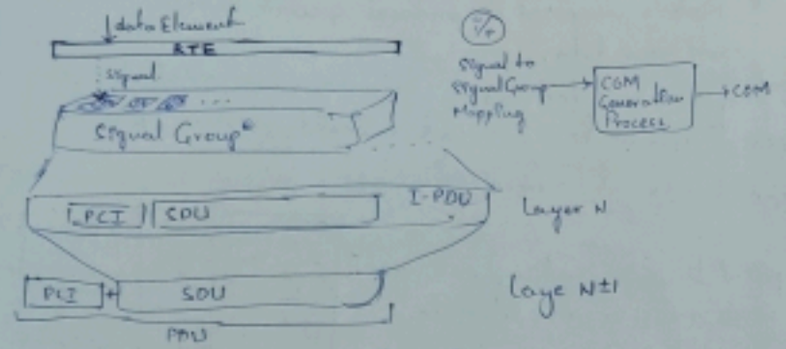
(n) Resulting RPN.

- After preventive/corrective action has been taken record Sev, Occ & Det^n

API	Pot^n Failure mode	Potential Effects	Causes	Current Prevention	Current Detection	Safety Measure	Recommended Action taken
ActivateTask (TaskType <TaskID>)	Input parameter recvd is already corrupted / TaskID by app^n is corrupted & within range	Intended task not activated, corrupted TaskID activated unintended task.	App^n needs to use Prog. Flow monitoring feat of wdg (Recommended ac^n)			use wdg Prog. Flow monitoring	*Add in Saf. manual
StdReturnType Rte_Write_p_o (data, Transformer Error)	Data Element corrupted & within range	Undefined	EMI Cosmic Radiation	AVIN Organization Design Guideline	Design review	*Config ECC feat. for RAM & Flash *E2E Protection	*Add in Saf. manual.
	Parameter passed by reference is NULL	RTE_E_INVALID_ARGS is returned to app^n	NULL reference	AVIN org. Design Guidelines	*Design Review *Existing Saf. mech. (DE validation)	App^n shall handle error detected & notified by RTE APIs	*Add^n SM in RTE module safety manual.
	Ref. given points to a loca^n that doesn't belong to the caller partition.	Pointer points to a loca^n that does not belong to caller partition	Pointing restricted memory Partition	-"-	*Design Review *ESM Segmentation viola^n Handling		-"-
	OS API call fails (ActivateTask(Id), SetEvent(OsTask, OsEvent))	RTE_E_OS_ERROR returned if OsTask returns other than E_OK	*Diff TaskID Corrupted TaskID	-"-	-"-	-"-	-"-

Implicit → works on a copy in our SWC (access array by means of a reference)

... RTE data.



* where do "signals" come from?

→ From SWC which are classified into 3 types.

(i) Sensor/Actuator S/wC → for handling sensor evaluation and actuator control functions (Specific ECU)

(ii) Composite S/wC → offers a logical interconnection (Many ECUs)

(iii) Atomic S/w C

FMEDA: (HARDWARE)

- SPFM – Reflects the effectiveness of the safety architecture to protect from residual faults (single point faults)
- LFM – Reflects the effectiveness of Saf. arch to protect from multi point faults.
- PMHF – Residual risk of a safety goal violation due to random H/w failures is sufficiently low.

Probabilistic Metric of

PDU Router: ← PDU Router routing tables + PDU Router Config

→ Func: – PDU receptions / Sending (transmissions) / Gateway

Routing PDUs between COM & CAN/LIN/FlexRay Interfaces.

I-PDUM: *To handle Multiplex messages on the CAN bus.

*To save CAN IDs by using more the one layout for one message.

14/12/19

CanTP protocol: (upto 4095 bytes)

* Sending more than 8-bytes of data over the CAN data frame which is not possible in normal CAN data frames limited to the only maximum of 8 bytes of the data.

* USED to transfer of diagnostic messages with OBD-II equipped vehicles.

* 1° task: Transfer messages that cannot be transmitted as single PDU due to their 'length'.

– Messages that are longer to fit in single PDUs are segmented by means of TP & divided into multiple, seperate PDUs.

Error handling:

* Both Tx & Rx monitors the data transmission with a timer.

Tx – monitors the time for the Rx to send the flow ctrl frame.

Rx – monitors the time reqrd by the Tx for sending Consecutive frames

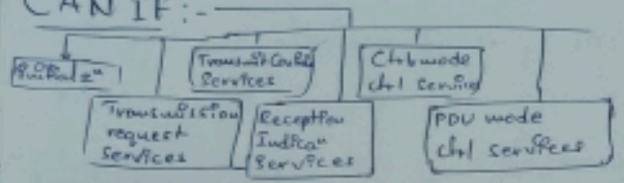
* Possible errors in the message structure are

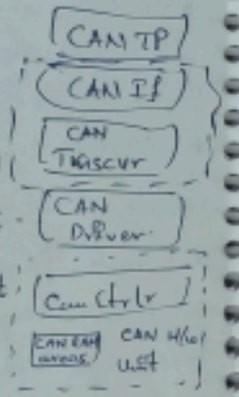
– Incorrect sequence number in consecutive frames

- Invalid message length
- Invalid flow status in flow ctrl frames
- Invalid PDU type

* Reassembles segmented messages at the Rx.

CAN IF :-





Notifies abt events (Rcp", Trsn, BusOff, Transmit Cancellation, Timeout) that occured in CAN controller

*Triggers interrupt

Can Trnsvr Drvr :-
- adapts the signal levels that are used on the CAN bus to dig. sig. levels recognised by a µC.
- Detects error - wiring issues, transmission of long dominant sig
- Abstracts CAN trnsvr h/w by using MCAL APIs to access Trnsvr h/w
- offers H/w independent interface to the higher layers

Item Definition :-

* Define and describe the item
- functionality, dependencies on, and interaction with the driver, environment & other items at the vehicle level.
- to support adequate understanding of the item so that the activities in subsequent phases can be performed.

HAZard Analysis and Risk Assessment :-

* To identify and classify the hazardous events caused by malfunctioning behaviour of the item.
* To formulate Safety Goals (SG) with their corresponding ASILs related to the prevention or mitigation of hazardous events, in order to avoid unreasonable risk.
* SGs and their assigned ASIL → determined by a systematic evaluation of hazardous events.
* The ASIL determined by considering Severity (S), Exposure (E) and Controllability (C)
* All done based on functional behaviour.

(a) Initiation of HARA

- Item w/o internal safety mechanisms shall be evaluated during the HARA.

E.g.: Electronic Stability Control (ESC) will mitigate effect of Brake Hydraulics System

(b) Situation Analysis and Hazard identification:

* Operational situations and operating modes in which an item's malfunctioning behaviour will result in a hazardous event shall be described

E.g.: Road condⁿ, weather condⁿ

↓

Correctly used | Incorrectly used

* Hazard caused by item's malfunction shall be defined at vehicle level.

* Hazardous events shall be determined.

* Consequences of haz. events

- Loss of the functionality of braking System (ESC) can lead to simultaneous unavailability of driver assistance functions.

- Loss of or failure of the vehicle's electrical power supply system can lead to a simultaneous loss of number of functions including "engine torque", "power assisted steering", "forward lights"

Goal: identify the potential unintended behaviour of the item that could lead to hazardous event.

(c) Classification of Hazardous Events

	S0	S1	S2	S3
	No Injuries (No ASIL Impl.)	Light and moderate Injuries	Severe and life threatening Injuries	Life threatening Injuries (uncertain survival) fatal Injuries
Classification / Freq. of Exposure	E0	E1	E2	E3	E4
	Incredible	Very low Probability	Low Probability	Medium Probability	High Probability
	C0 Controllable in general	C1 Simply Controllable	C2 Normally Controllable	C3 Difficult to control or uncontrollable.	

QM – quality processes are sufficient to manage identified risk.

(d) Determination of Safety goals

- SG – for each haz. event with an ASIL evaluated in HARA.

∴ Similar SG – combined → Highest ASIL considered.

(e) Management of variances of TSR in hazard analysis & Risk assessment

- Vehicle specific configuration shall be specified

E.g.: Tractor with trailer provides vehicle dynamics stability via drive axle.

(f) Verification

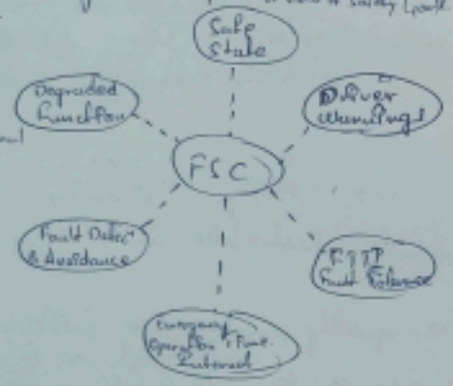
– In accordance with part 8 clause 9. to provide evidence for the:

* Compliance with
  - Haz. events
  - SG and ASIL

Functional Safety Concept:

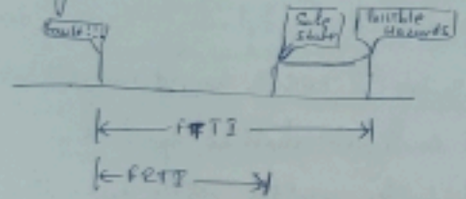
(a) Derivation of FSRs:-

* operating modes
* FTTIs
* Safe states
* Emergency operation time interval
* Functional redundancies



* e.g. Switched off, locked, reduced functionality
* presence of Safe & Safety Goals

FTTI: time span in which a fault or faults can be present in a system before a hazardous event occurs.



* If safe state cannot be reached by a transition within an acceptable time interval, an EMERGENCY operation shall be specified.

* Driver actions shall be specified in FSC.

E.g.: ACC generated brake actions being overridden when the driver presses the accelerator pedal.

* FSR shall be allocated to the elements of the system architectural design (ASIL & Safety Goal wise)

* Each Safety Goal – at least one FSR.

* FSC – shall consider
  - Element of other technologies
  - External measures.

(b) Safety Validation Criteria:- (upper right of the V-Cycle)

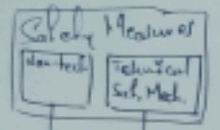
– The acceptance criteria for safety validation of item shall be specified based on the FSR & Safety goals.

(c) Verification of functional safety concept:

– the consistency & compliance with the SGs: &
– the ability to mitigate & or avoid the hazards

E.g.: by tests, trials or expert judgement, simulations.

→ addresses characteristics of faults: Transient, Permanent.



→ E.g: Error Correcting Code (ECC)
Cyclic Redundancy Check (CRC)
H/w redundancy
Built-in-self-test (BIST)

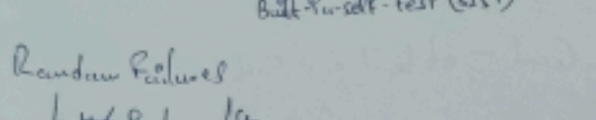
Random Failures
- ~~H/w~~ Systematic
- Random H/w
  - Permanent faults (stuck-at faults)
  - Transient faults (single-event-upsets, soft errors)

* Safety mech to detect Random H/w failures
  - ECC, CRC, H/w Redundancy, Built-in-self-test
* Three metrics to detect fault and failure in time (FIT)
  ; The effectiveness of the safety mech to detect Random failures
  - Single-point fault metric (SPFM) - robustness to single-point faults
  - Latent fault metric (LFM) - multi-point faults not detected by saf. mech
  - Probabilistic metrics for H/w failures (PMHF)

Source for Random H/w faults

EMI | Cyber attacks | Cosmic radiation | Voltage variation

(E.g. gates stuck at wrong value)



* How fault is causes interference b/w swcs & what are possible prevention/detecting mechanisms.
→ Faults that cause interference b/w swcs are;

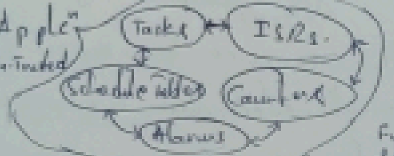
Memory | Timing | Exec° | Exchange of Information

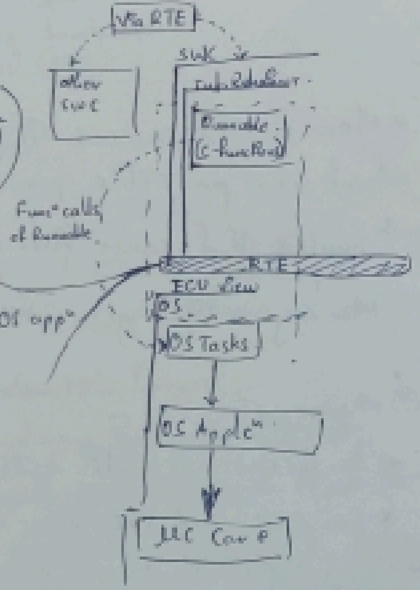
① Memory:
* An ECU — all diff. ASIL swc (Safety related/Non-Safety related)
* Low ASIL rated swc may interfere by wrongfully accessing memory regions of other swcs with a high ASIL rating.
* The feature of mem. partitioning should help swcs to prevent interference by partitioning mem. for swcs with respect to ASIL levels, & facilitated by OS & RTE functionality.

FSM:- Memory Partitioning (One Partition implemented using one OS appl" memory)

* by means of protecting of restricting access to memory and mem. mapped H/W.
* means OS Appl"s reside in different mem. areas that are protected from each other.

* OS Appl": Trusted / Non-Trusted

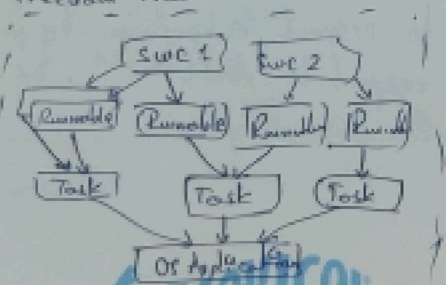




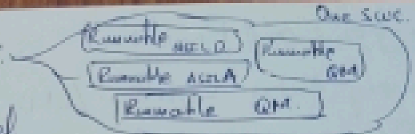
Runnable mem. area that is accessible by all members of OS app" with facility to comm" b/w SWCs.

(a) within App" S/W

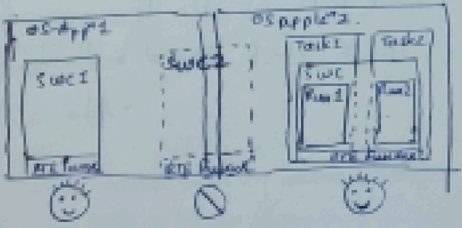
* Mem. Parti" – does not provide "freedom from interference" b/w SWCs within one OS Applc".
* Faulty SWC would modify a mem. area of other SWC within one OS applc".



(b) Within S/W Components:



* Mem. par" done at OS-Applc" level cannot be used to separate Runnables within the same SWC. Hence, Task level partitioning.



* Req E.g": "The OS module may prevent write access to the private stack of Task/Cat 2 ISRs of a non-trusted applc" from all other tasks/ISRs in the same OS Applc."

Implementati of Mem. Part'ing:

* Memory Protec" Unit – supports Mem. Par" via dedicated H/W.
- write access to RAM may produce memory corruption
- Peripheral-Reading from peripheral address space

E.g: "Acknowledgment of a Interrupt done via a read access to interrupt ctrlr may cause I/O errors."

*

Detection and Reaction:

* Memory Access Violation/CPU Instruction violation in a non-trusted partition the faulty access is blocked & an exception is raised by which ~~the~~ H/w.
  - OS & RTE handle the erroneous s/w partition by performing
    [partition shut-Down] or [restart] of all SWCs of this partition

(ii) Timing.

FSM: Timing Monitoring

* Fault Models (Timing & Execution related faults that cause interference)
  - Blocking of execution
  - Livelocks
  - Deadlocks
  - Incorrect alloc of execution time.
  - Incorrect synchron b/w SW elements.

* Timing Protection & Monitoring is monitoring ~~of the faults~~ that tasks are dispatched at the specified time, meet their execution time budgets & do not monopolize OS resources (such as tasks having heavy CPU load, many interrupt reqsts)

* Timing monitoring mechanisms by AUTOSAR
  - Timing Protection mech. using the OS.
  - Temporal Program Flow monitoring using WdgM.
    - Alive Supervision
    - Deadline supervision.

* Supervise Entities can be — SWCs / Runnable in SWC / BSW module / CDD

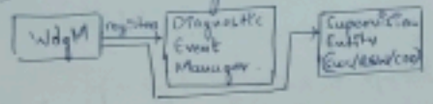
* checkpoints - important places in a supervised entity.
* code of supervised entities - interfaced with func calls of WdgM.
* those calls are used to report to the wdgM that a checkpoint is ~~reached~~

Alive: * Periodically checks if the checkpoints of supervised entity have been reached in given limits
- checks if a supervised ent. is run not too frequently or not too ~~early~~ rarely.

Supervision of S/w execution → WdgM → (triggering) → Watchdog Hardware

* Error Recovery Mechanisms by WdgM:-

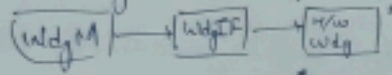
(i) Error Handling in the Sup. Entity.



(ii) Partition Shutdown:

* Failure in a Sup.E in non-trusted parts", WdgM may request a partition shutdown by calling the BswM.

(iii) Reset by H/w Watchdog:



* resets the ECU / MCU / complete SW.

(iv) Immediate MCU Reset

* Short global reacn to the supervision failure if necessary, the WdgM may directly cause an MCU reset.

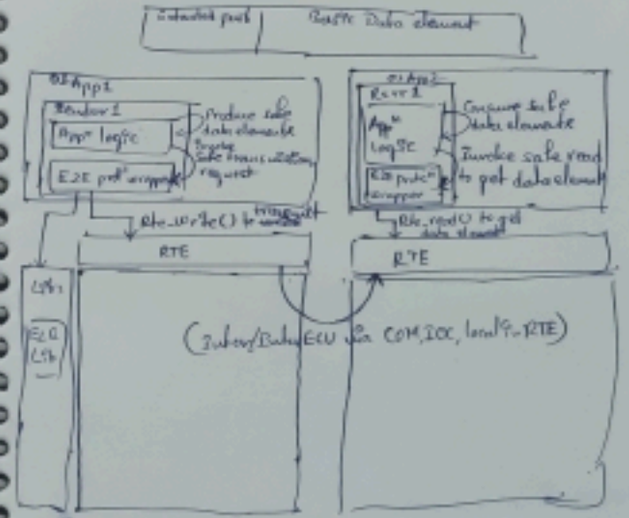
- Re-Initialz" of MCU H/w & the complete S/w.

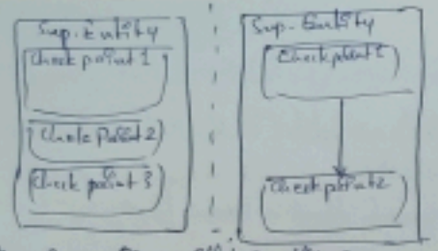
End-2-End Protection:

* Safety-related data exchange shall be protected at runtime against the effects of faults within the communic" link.

Faults e.g.: * Random H/w faults (Corrupt registers of a CAN Transceiver)
- Interference (due to EMC)
- Systematic faults within the s/w implementing VFB communic" (RTE, IOC, COM & N/w stacks).
Inside the ECU or Gateways (outside)

* Extends data element with Counter, Timeout, Data ID, CRC





After Supervision with; Deadline.
Independent checkpoints; Supervision

Deadline:

* Aperiodic/Sporadic monitoring b/w two checkpoints that has individual timing constraints.
* WdM - checks if same steps in a supervised Entity take a time that is within the configured minimum and maximum.
* If the second checkpoint is never reached, the Deadline Supervision will fail to detect this error.
This error appear because the timing checks are performed by the WdgM after the second checkpoint is reached

Timing Protection:

* Timing fault - a task/interrupt misses its deadline runtime.
* Tasks/Interrupt missing deadlines are determined by:
  - Execution time of Task/Interrupt
  - Blocking time that Task/Interrupt suffers from lower priority by T/I locking shared resources / disabling interrupts.
  - Inter-arrival rate of Task/Int.
* Timing Protection Mech by AUTOSAR OS.
  - Exec Time Protexn - Upper bound for execution time (Execution Budget)
  - Locking Time Protexn - Upper bound for blocking of resources, locking & suspending of interrupts (Lock Budget)
  - Inter-Arrival Protexn - A lower bound b/w tasks being activated or Cat 2 Interrupts arriving (Time Frame).

Detection and Reaction:

* Based on results from each enabled monitoring/protection mechanism, the status of SE (local status) is computed.
- Then Based on each local Supervision status, the status of whole MCU is determined (Global Supervision Status)

Perception Phase Terminologies:

* Proprioception → acquire data related to internal state of the vehicle.

E.g.: GPS, IMU, Gyroscopes, wheel speed sensors, compasses.

* Exteroception → acquire data abt external environment around the vehicle.

E.g.:- Radar, Lidar, Camera, Ultrasonic.

* Different Protection Error in AUTOSAR OS:-

- mem. access violation:- A "protection" error caused by access to an address in a manner for which no access rights
- Timing fault:- A "post" error that violates timing protection.
- Illegal service:- —"— violates the service protection
  e.g.:- unauthorized call to OS service.
- H/w exception:- Division by zero, "Illegal instruction" etc.

* OS Task:- It is the object which executes user code & which is managed by OS.

E.g.: OS switches b/w different tasks.

Two types
- Basic Task - W/o Waiting state.
- Extended Task - W/ Waiting state.

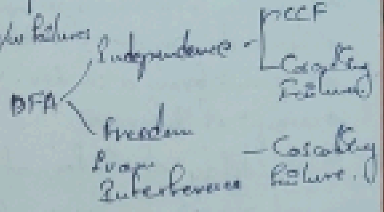
* Hazard Example.
  - Driving or stopping with a too low longitudinal distance to a static or dynamic object or undriveable region ahead
  - Driving faster than situation velocity or ego sight allows.
  - Missing reaction to passenger request or interactions in SDC.
  - Not granting passage to emergency vehicles before coming to a stop.

* Safety Goal Example
  - Avoid driving or stopping with a too low longitudinal distance to a static/dynamic object or undriveable regions ahead.
  - Avoid driving faster than situational velocity limit or ego sight allows.
  - Avoid missing reaction to passenger request or interactions in SDC
  - Avoid not granting passage to emergency vehicles before coming to a stop.

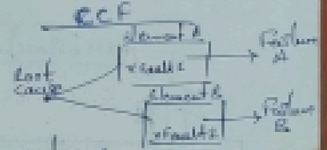
* Functional Saf. Req:-
  - The LiDAR shall avoid or indicate E/E faults that lead to an incorrect 3D point cloud.
  - the LiDAR shall avoid or indicate E/E faults that lead to detection of physically non-existing objects (Ghost objects)
  - Front Light Management (FLM) shall detect any valid turn ON condition of low beam correctly (ASIL B)(MF: No [illegible] of a 'ON' req.)

* [illegible] shall provide a mechanism to reach [illegible] position [illegible]

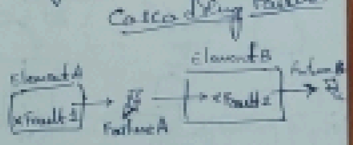
Dependent Failure Analysis (DFA)
- To identify failures that may hamper the required independence or freedom from interference b/w given elements which may lead to violation of Safety goal / Req.
- Systematic failures & Random h/w failures



- Dependent failures can be identified by
  - Deductive (FTA) analysis
  - Inductive (FMEA) analysis



- Plausibility checks - ~~[illegible]~~ checks to prevent attacks on safety critical systems. shall be considered.



Freedom From Interference (FFI):-
- Analyzing interference b/w elements
- for possible failures like
(i) Timing and Execution:
  * blocking of execution
  * deadlocks - several processes blocking mutually by waiting for events that can be triggered by themselves
  * livelock - several processes keeping each other in infinite loops
  * incorrect allocation of execution time.
  * incorrect synchronization b/w s/w elements.

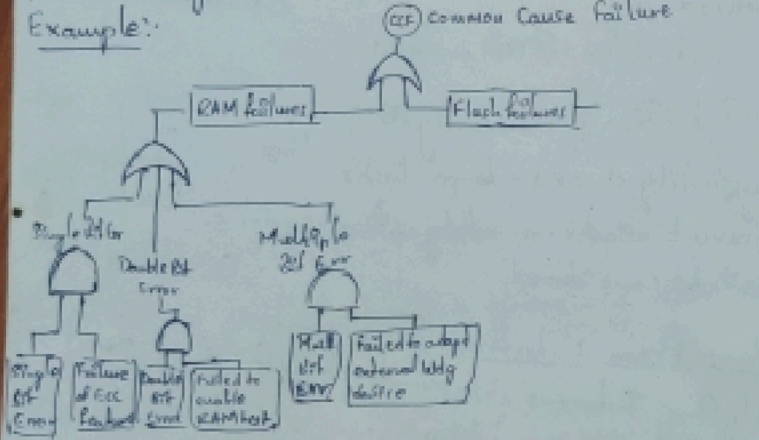
(ii) Memory:-

* Corruption of content.
* read or write access to memory allocated to another s/w element.

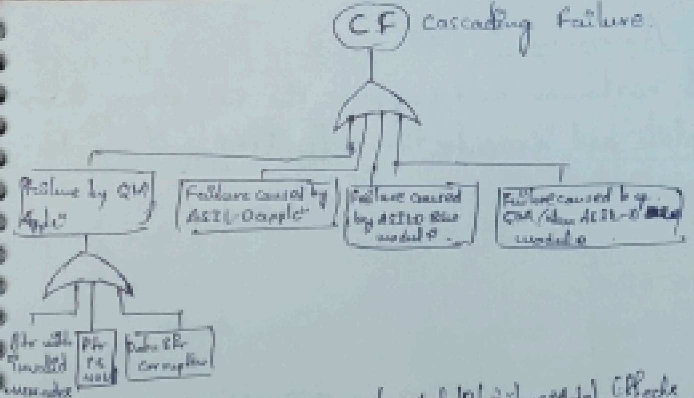
(iii) Exchange of Information:-

* Repetition of information
* Incorrect sequence of informa^n
* Information from a sender received by only subset of receiver.
* corrup^n of informa^n
* loss/delay of information.

Example:-



Module	Root Cause	SW Dependency	Dep. Failure Mode	Pot. Fail Mode	Effects	Saf. Measure
RTE	Random H/w failure	Shared H/w Resource	Single/double/Multiple bit errors	Single/double/Multi bit errors	Multi bit err corrupting RTE internal data structures	ECC & RAM Test



Module	Root cause	SW Dependency	Dep. Failure Mode	Pot. Failure Mode	Effects	Saf. Measure
QM/Non ASIL-D Applic^n	Systematic Factor	Shared SW Resource	Data buffer corrupted	Non-ASIL applic. [illegible] data buffer corrupted by ASIL B/C/D application.	Undefined	Configure ASIL A/B/C/D in [illegible] separate memory partition.

Fault Tree Analysis:-

1. Define the system.
2. Define top level fault(s)
3. Identify causes for top-level fault
4. Identify next level of events
5. Identify root causes
6. Add probabilities to events.
7. Analyze the fault tree - identifying single/multi point faults.
8. Document the FTA.

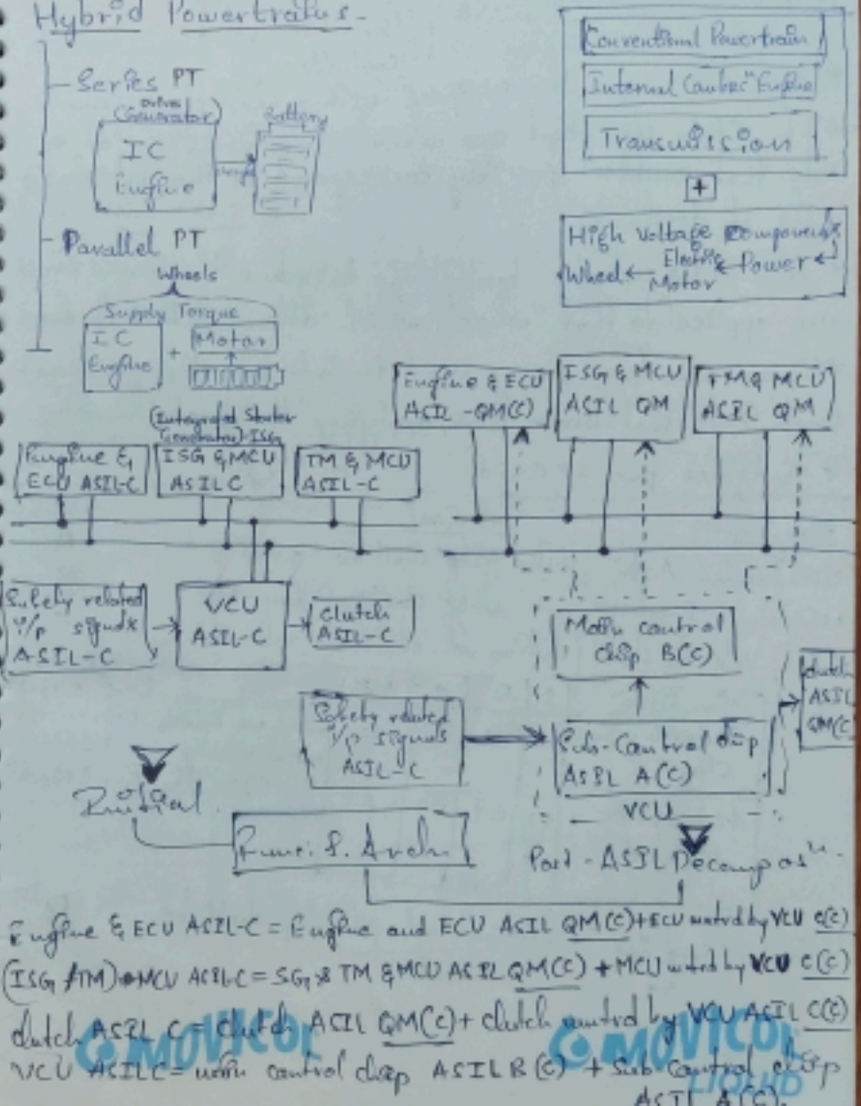
*Dev. Interface Agreement (DIA)

Provide both customer and supplier the necessary inputs to properly plan and execute the activities and work products

8-9/01/2020

Hybrid Powertrains -

- Series PT
- Parallel PT



Engine & ECU ASIL-C = Engine and ECU ASIL QM(C) + ECU monitored by VCU C(C)

(ISG & TM) & MCU ASIL C = SG & TM & MCU ASIL QM(C) + MCU monitored by VCU C(C)

clutch ASIL C = clutch ASIL QM(C) + clutch monitored by VCU ASIL C(C)

VCU ASIL C = motor control chip ASIL B(C) + Sub-Control chip ASIL A(C)

Anti-Lock Braking System
- 4 Wheel speed sensors
- 1 Hydraulic pump
- 1 Hydraulic valves.
- Controller.

* Controller monitors speed using wheel speed sensors.
* If Ctrlr sees that one wheel decelerating at a rate that could not possibly correspond to the Vehicles rate of deceleration.
* Actuates wheel's brake line to reduce the brake pressure applied to that wheel. which allows to turn faster.
* Once speeder, pump used to introduce the pressure back into that brake line, applying that brake again.
* 15 times per second.

Haz Event	Saf. Goal.	ASIL
Unintended Accln	Unintd. Accln shall be avoided	A
unint. — Deceleration — decln shall be avoided		B
Unintd. Vehicle start	Unintn veh. start. shall be	C

Oper. Situation	S	E	C	ASIL
Entering Bus stop	S2	E4	C2	C
At traffic light	S1	E4	C2	A

* driver TTR = 1.5s
* considered accelⁿ of 2.13 m/s²
which veh. travels s = 2.9m and at velocity = 11.5 km/h.
* Collision b/w Bus & Pedestrian

Unint. Sideslip	Unintd. vel. sideslip shall be avoided.	B

Electronic Stability Control. (ARS Sensor + Yaw sensor + Acclrmtr + steering angle sensor.)
↳ computed control sys that applies brake to individual wheels and reduces engine power to ensure driver ctrl on vehicle (mostly use case in Turning).

Traction Ctrl :-
If vehicle is unable to gain traction in icy conditions, one wheel will spin while the other simply remains stationary.

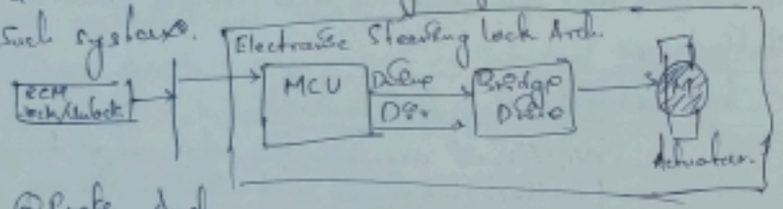
Control Unit	Saf. Req. / Saf. Functions
VCU	- VCU shall monitor the total wheel torque against maximum and minimum limits. - VCU shall monitor the actual torque of TM against the request torque. - VCU shall monitor actual gear/accelerate /break pedal position

Metric	ASIL B	ASIL C	ASIL D
Single Point Failure Metric	>90%	>97%	>99%
Latent point failure Metric	>60%	>80%	>90%

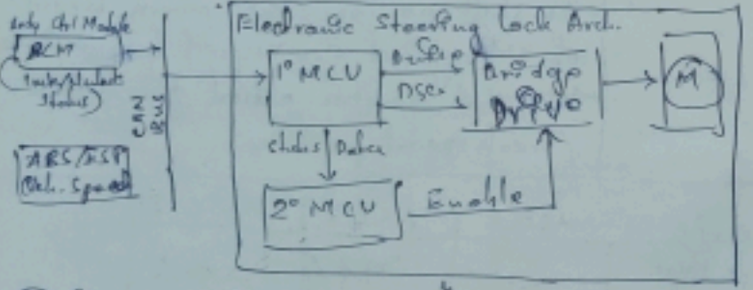
MOVICOL LIQUID

ASIL Decomposition:

* For ASIL-D systems that demand the highest levels of diagnostic coverage, it becomes very important to ensure that a single sys. fault doesn't lead to a complete catastrophic loss of function.
* Decomposed architectures help achieve this goal & can be a critical design option when developing such systems.

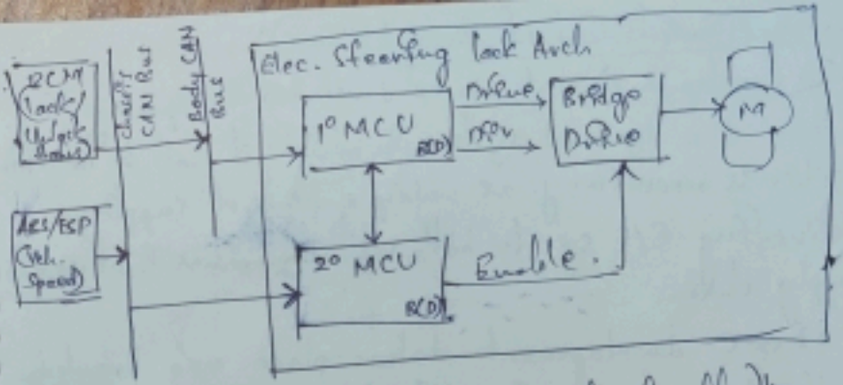


(a) Prefer. Arch.



(b) Flawed ASIL Decomposition.

* A common cause failure on 1° MCU could result in incorrect veh. speed pulses being transmitted to 2° MCU. which violates safety goal.



Advantages:- (More reliable & robust path) hop

* Can be used existing components like an ASIL B/QM MCU to implement a higher ASIL-D system.
* Diff. ASILs combined
* Dual channel - helps with functionalities when there is repairs / System recovery.
  - advantage of choosing MCUs based on strength of each function (Real time Control & Safety/Security purpose)

Safety Element Out of Context (SEooC):

- To develop an element can be developed independently from the top-level system in which it shall be integrated.
- This is necessary as multiple types of suppliers delivering E/E sys to both veh. manufacturer & others in supply chain.
- SEooC development takes place w/o knowledge of the design or requirements from the top-level system, so from beginning of the development process assumptions are made abt the item the SEooC shall operate in, and the applicn it shall be used within.
- SEooC will be designed to be capable of complying with assumed requirements of a certain ASIL.

- To consider & document :-

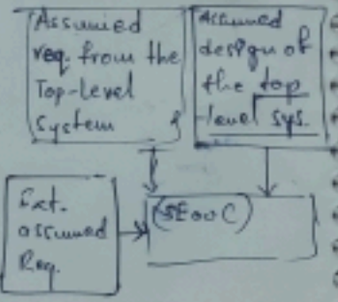
(i) To derive FSR, make assumptions about top-level sys.

(ii) Boundary of SEooC.

(iii) Readable format
- full traceability to assumptions

(iv) assumed req. to be considered while carrying out Safety Analysis or DFA.

- Confirmation based on assumed req. should be



In edition 2 (2018), SEooC in terms of semiconductors has been explained.

WSS - Wide Sense Stationary Signals