التاريخ: / / الموضوع

Automotive Functional Safety
ISO 26262-2011

 # What is Safety ?

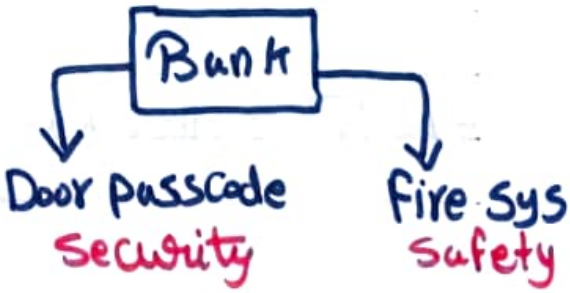
→ State or a place in which you are Safe. (تكون) قضاء وقدر.. أو بسبب خطأ بشري

→ Safe system which in not cause any protictional risk

* Safety Critical system →
  لو حصلت أي مشكلة ممكن تسبب ضرر كبير ويمكن قاتل
* Non-Safety Critical system →
  لو حصلت مشكلة ممكن تتحل وتبقى ضرر.

 # What is Security ? قضاء وقدر برضو بس بسبب الشر النفس البشري

→ Protect — Person / organization / building against crime or attacks (متعمد)



 # Functional Safety :

→ Focus on how the system's functionality fail in a safe way & reduce the risk that can be caused by a system when it's function fails

Functional Safety Standard IEC 61508 "General"

* Standard published by the international electrotechnical Commission
* Consist of methods on how to { design, deploy, maintain } automatic protection systems (safety related systems)
* This standered aplicable to all kinds of industry

الـ Functional Saf- نقدر نعتبرها جزء من نظام الـ Safety control اللي بتتحكم equipment under control اللي بسميها EUC
Safty systems ← E/E/PE على الـ

E/E/EP : electrical / electronic / Programmable electronic Safety related systems.

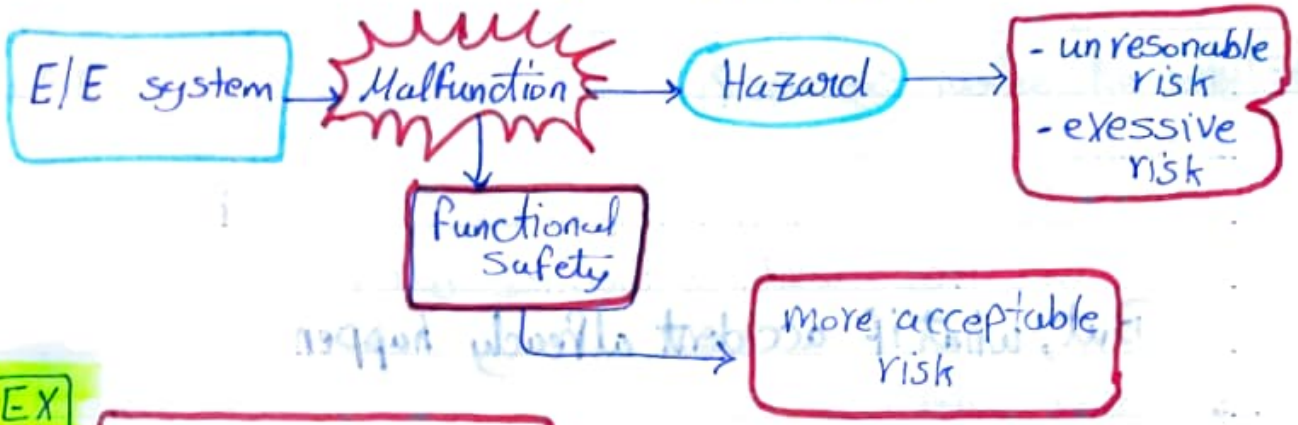
→ now for automotive industry there Standered specific for it [iso 26262]
this standered cover all development process
- requirements specification
- Design
- implementation
- integration.
- Verification
- Validation
- Configuration.

→ not related to mechanical systems.

→ For iso 26262 .. functional safety is absense of unresonable risk due to hazards caused by malfunctioning behaviour of electrical/electronic systems.

electrical / electronic } أي خطأ غير متوقع يحدث بسبب خلل في الـ H.W سواء كان

والخطأ ممكن يتسبب في كارثة [hazard]:



EX

Adptive control system → Malfunction

Malfunction → no control on acceleration then, high speed will lead to accident

Malfunction → - But by iso 26262 you will some steps "safety steps" to reduce the risk
- you can still detect & control this malfunction.
- The risk will be at acceptable risk

How the Functional Safety Lower the risk.?

① identifying hazards حدد المخاطر

② Measuring associated risk نقوم بتقييم المخاطر والمخاطرة في كل قرار

③ Lower the risk to an acceptable or resonable Level

نختار الـ risk الي هيقلل الـ risk لأقل خطر وأكتر مخاطرة مقبولة

Types of safety systems?

→ Active Safety :

Safety system that help to avoid any accident like ABS "Antilock Breaking System".

But, what if accident already happen

→ Passive Safety :

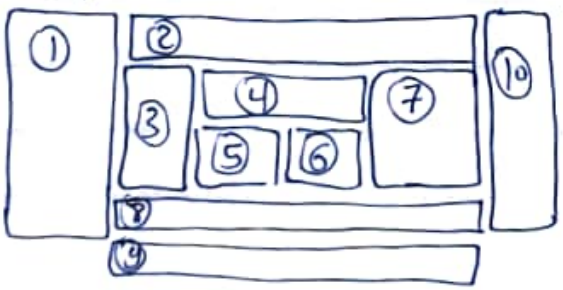
Safety system that help to reduce the effect of an accident like "Air Bags"

ISO 26262 consists of 10 parts they have two main categories

Cat(1) → Normative parts : هي مجموعة من المعايير اللي بنمشي وراها عشان نوصل لمتطلبات النظام من الـ Safety المناسبة

Cat(2) → informative parts : هي عبارة عن وصف للحلول الموجودة في كل مجال من المعايير اللي تم الإستدلال لها في [normative parts]

System shape

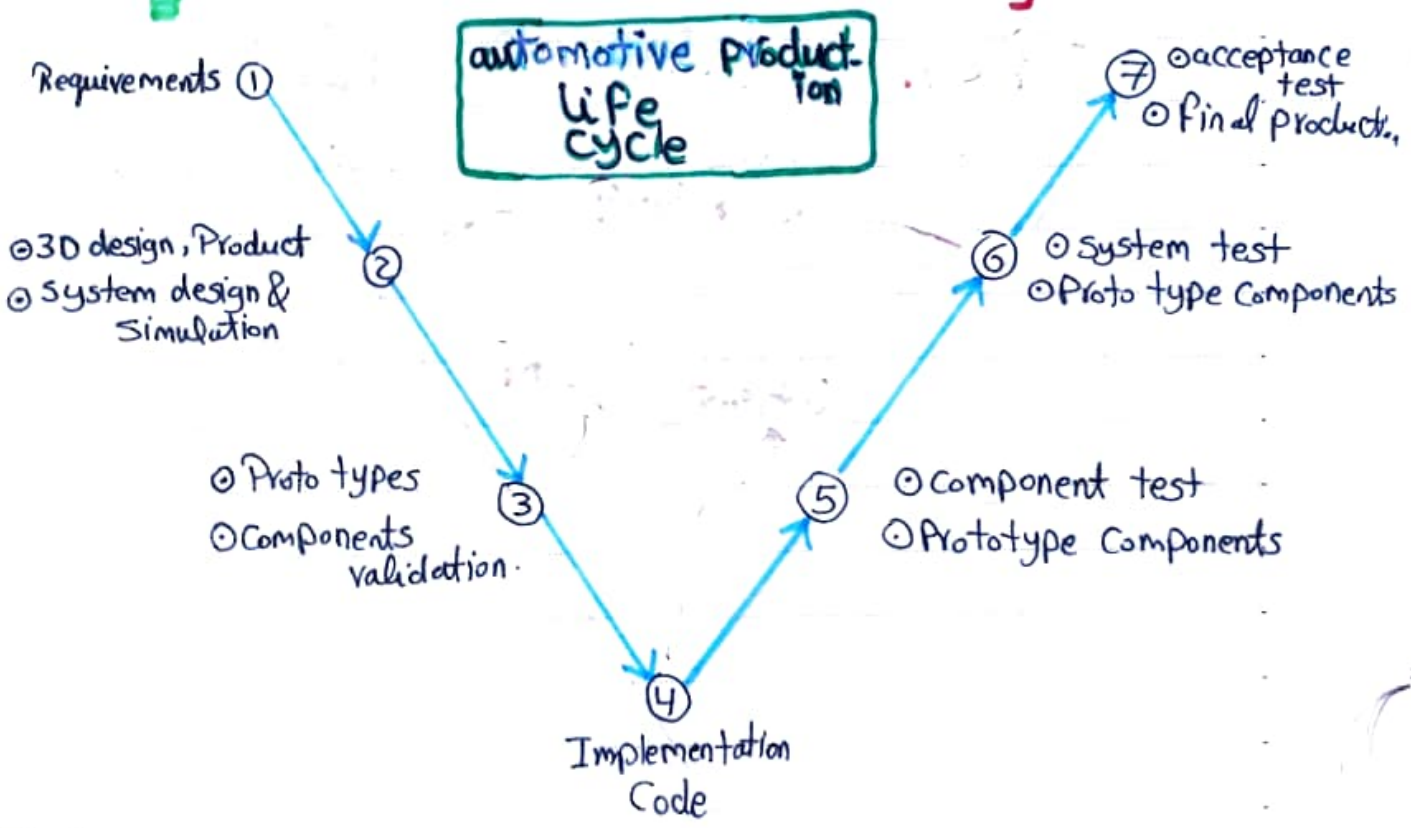


Part (1): Vocabulary: "Dictionary of the iso"
contains definations for application in all parts of the standard.

Part (2): Management of Functional Safety:
- what are safety requirements from project.?!
- خلالها نقدر نطرق معايير المتطلبات لل safety و إزي هم بيطبق
- Safety management during item development الـ safety life cycle لأن منتج في الـ automotive

Part (3): Concept phase:
" (4): Product development at the system level:
" (5): " " " " hardware level:
" (6): " " " " Software ":
" (7): Production & operation:

These 5 parts could be presented as testing "V" model.



Part (8): Supporting Process:

في جزء Safety process بتتكلم الـ safety life cycle

- Distributed development
- Verification
- Documentation
- Qualification of SW tools
- Qualifications of [H.W / S.W] Components

Part (9): ASIL-oriented and safety-oriented analyses:

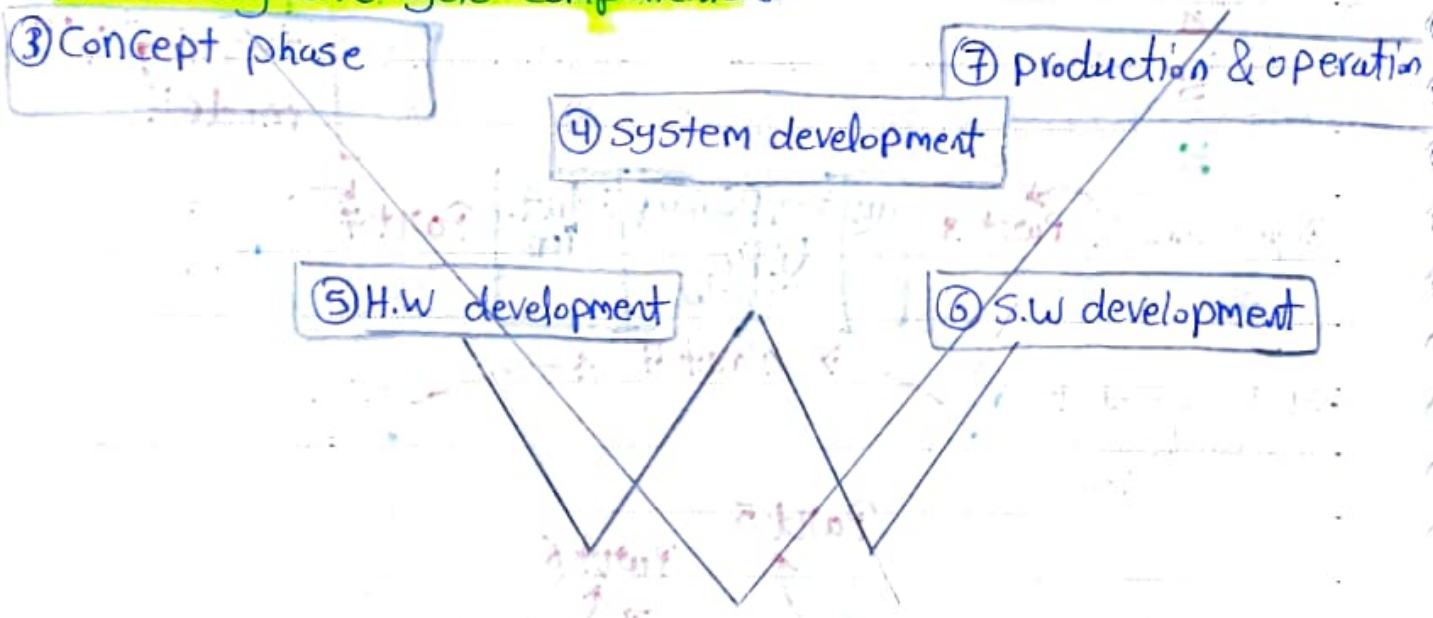
في Guide بيكون وصف للخطوات بتاعة الـ Safety اللي تم تنفيذها للشروع بيها

- requirements analysis
- Safety analysis
- Analysis of dependant failures.

Part (10): Guidline on ISO 26262:

وصف الـ Standard المستخدم في الـ Project.

Safety life cycle Components:



Concept-Phase
① item defination
② initiation of safety life cycle
③ Hazard & risk analysis
④ Functional safety concept

③ Concept phase:

① * at the first : before design & implementation we need to know [item defination] like features of the car & functionality of each, we can say item is an e/e system or collection of them that have function. or some functions

* There some info you need to know about the item begaining from Perpose, functionality & how it depend or communicate with other items.

* item defination document : يحتوي على وصف الـ item وطريقة العمل والظروف التي يتم تشغيل فيها وأعتمادها على الـ items الثانية

* EX: in automotive project there "item defination document" for anty lock breaking system , Adptive cross control, ---

* objective of item defination:
  - describe items & it's dependancy on other items

② * Initiation of safety life cycle.

- ⊙ in this step you have to decide for any item if it new or development to an existing item, if this a development of existing item you have to make impact analysis " تحليل التأثير " that to see what will be affected by this modification.
- ⊙ initiate safety life cycle. after modification.
- ⊙ To implement functional safety in automotive software development you have to ~~implement~~ plan safety steps then implement them.

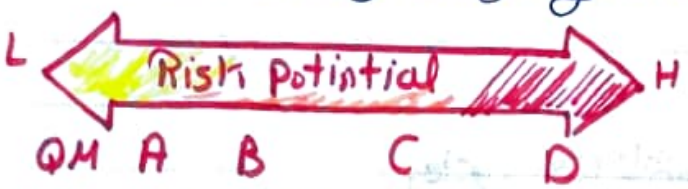
⊙ To start 'safety Life Cycle. you need to generate two things
Ⓐ impact analysis : • what is affected due to item modification.
Ⓑ Safety plan : to achive functional safety we should know what should be included in the safety plan, which item for which activity

③ Hazard analysis and risk assessment (HARA):

⊙ analyze item to find possible hazzards.
⊙ then risk assessment .. study how much hazard is risky..

- في الخطوة دى بنشوف كل item إيه المخاطر المحتملة اللي موجودة فيه وكل خطر منهم إيه الـ risk الموجود فيه
- بعد تحديد مستوى الخطورة بيتم تمثيل مستوى الخطورة بـ ASIL

ASIL → automotive Safety Integrity level (ASIL)



- المستوى اللي بيتم تحديده من خلال ASIL من خلال حسابات وعلاقات بيتم تحديدها في الـ iso standard وده بيعتمد على مجموعة من العوامل منها
  - الخطورة
  - قابلية الإنفجار
  - التحكم بحيث يقلل الـ failure

  والهدف هنا إننا نقلل الـ risk لمستوى مقبول

- in this step no need to know detailed design of item as it depend on the over all analysis of the functionality for this item

St.1

① Hazard analysis :

→ Find out hazards caused by malfunction behavior.

Ⓐ Identify the Functionality (Function list)

~~for each item there some Function list~~

كل item موجود بيكون ليه ما يعرف بـ Function list يعني مجموعة من المهام اللي هو يقوم بيها

Ⓑ Functional Failures

* ممكن يحصل عطل في واحدة من المهام بتاعة الـ item وكمان لازم تكون عارفلينها بناءً العطل عطل كامل و لا عطل جزئي ولا عطل بسبب تعرف غير مقصود من التحكم نفسه

Ⓒ Hazard defined at the vehicle level.

بعد ما يحصل العطل .. ما هي المخاطر المترتبة عليه وما هي الحادثة المتوقعة

St.2

① Risk assessment :

من: هنا نقدر نحدد مستوى الـ risk على ASIL من خلال معادلة فيها ٣ عوامل أساسية هم:

exposure ←
severity ←
Controllability ←

Risk = Severity(S) * Controllability(C) * Exposure(E)

exposure(E)

How much it could be happen

بتتكلم عن الفرصة المحتملة لحدوث الـ risk بتحصل بنسبة كبيرة و لا صغيرة

- E0 never
- E1 rarely
- E2 sometimes
- E3 Quite often
- E4 often - always

Controllability

measure how much I able to contol the car while hazard

- C0 controllable
- C1 Simple Control
- C2 normally control
- C3 difficult to control

Severity

how badly person can get injured } how hazard can be harmfull } S0 no injury
S1 moderate injury
S2 life thrating
S3 fetal injuries

ASIL : Automotive Safety integrity level. مستوى سلامة المتطلبات

at page.8 graph shows the levels of ASIL

ASIL(A) ------------------ ASIL(D)

Low Hazard	high Hazard.
"Some requirements which are applied to ASILD are here could be optional"	"Very resky item there we need so meny requirements to make sure of safe functionality"

The level called (QM) "quality management level"
↳ "not safety related item" ⟶ But that dose not mean no need for safety requirements
↳ ولاكنه يمكن تطبيقه اى standered لل safety من شروط ال iso 26262

The iso 26262 provides table for three factors & they are corresponding to ASIL level

بنشوف ال item ونحدد ال 3 factors ونشوف موقعها في الجدول ونحدد على ال ASIL

→ Now after find out the level on ASIL .. indicate the requirements for this level which beside them we find some signs

++ ... highly recommended

\+ .. just recommended.

0 -- not "

notes

\# ISO 26262 allow us to reduce the ASIL level to lower level using ASIL decomposition → يعني لو ال item واخد مستوى عالي ASIL

→ divide this item into 2 system are independant → كل system منهم له ASIL level أقل

EX 1

| Main item | ASIL | D |

- System(1) ASIL B(D)
- System(2) ASIL B(D)

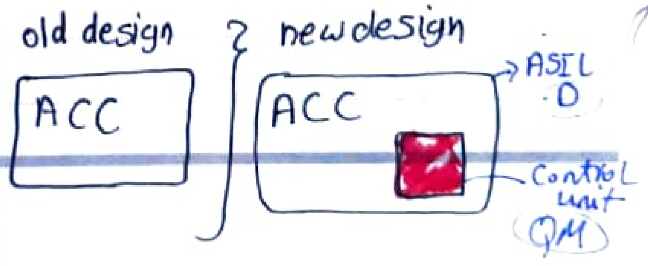
or

- System(1) ASIL D
- system(2) QM

EX 2

ACC ⇒ ASIL D

instead of this item has ASIL D level we will make individual safety Controller inside this item if there any mistake in calculations this controller will solve the problem



St.3

Safety goals:

تمثل هذه المرحلة الـ Requirements الرئيسية لكل item وهي تحدد السيناريو الذى يجب إتباعه لإستبعاد أى hazard من المتكررة

يعني بنشوف الـ item يقدر يعمل إيه في حالات معينة وندرس الـ hazard والـ risk اللي مترتب على حاجة زى دى وبعد تحديد مستوى الخطورة لأى function يقدر الـ item يعملها نقدر نلخيها لو مستوى الخطورة بتعها عالي نسبيًا

At the end of ~~Haz~~ HARA we can say et it's output depend mainly on two Things → Safety goals, ASIL determination. "Level"

④ Functional safety Concept:

- it is the last phase of concept Phase which is the first step of safety life cycle.

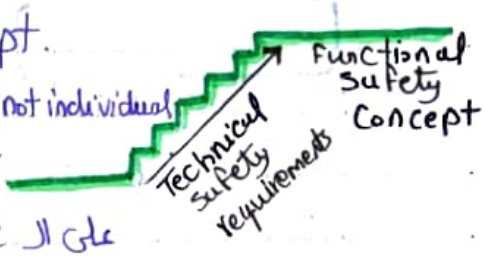
في الخطوة دى بنشوف الطريقة المناسبة عشان نطبق طريقة Safety معينة والي هتحقق الـ Safety goal وطبعًا الطريقة دى ليها مجموعة من الـ requirements اللي بتتوافق مع الـ ASIL level عشان نشوف إيه في الـ reqs دول لازم يتعمل و اى منهم إختياري

(4) Develops System Development:

① Product development at System Level:

* ايه في الـ requirements اللي سمعنا عنها قبل كده وطريقة الـ function Safety Conc.

* OR, we can say what are Technical safety requirements او نقدر نقول on the system level "more details" that are suitable to apply Functional safety Concept.



* on System level means [items integration] not individual

* ولكن مش كل الـ Requirements لازم تكون بتتعمد على الـ safety Conc وده هشام في بعض العوامل الخارجية اللي ممكن تؤثر لنفس الـ malfunction والـ safety concept من حاطوها في الإعتبار لأنها مش بتتعمد على الـ item. ولكن بتتعمد على العوامل الخارجية زي مثلاً memory Corruption و Communication bus failure

والعوامل اللي ممكن نكتشفها سهلة { ما يعرف بـ Safety analysis

* Safety analysis:

- way to discover possible fault in the architecture that can distroy safety goals.
- This analysis can be don on software & hardware levels. that depend on architecture it self.
- methods: FTA , FMEA , FMEDA .
- Types of failures:
  - (A) Random hard ware: due to hardware elements failure & this type is unpredictable. [like: broken Connection]
  - (B) Systematic failure: due to deterministic cause & we can treat this failure by changing design or process

- Methods of Safety analysis: on System level

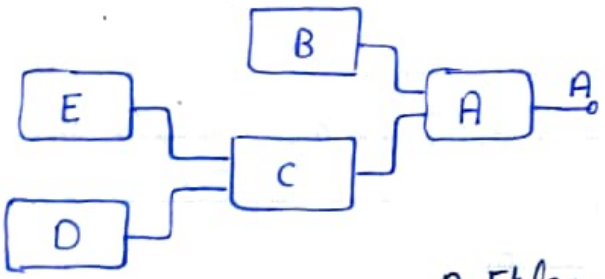
(A) FTA: Fault tree analysis: Logical method

من الطريقتين هي طريقة تنازلية بتقوم بتحليل الـ Fault لمجموعة من الأحداث أو الـ Faults الأقل والي هم في الأصل تسببوا في الحدث الأكبر وبعدها بتقوم بتحديث الـ design حتى تقلل الـ failures المحتملة

Steps of FTA

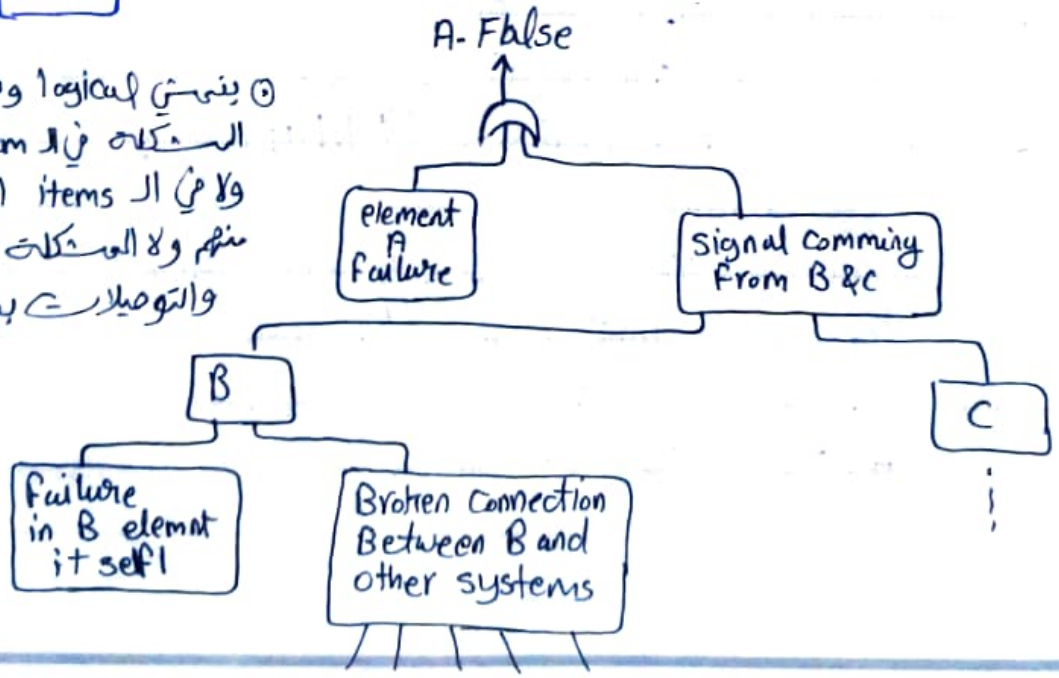
1. Top level event: Undesirable state of the system
2. start top down analysis: Fault لحتى نوصل لأسباب الرئيسية للـ
3. what is the suitable Safety mechanism for this Fault "event" & this mechanism expressed as: Safety requirement.

Example of FTA



⊙ if the output signal (A) is interrupted.. we should find out the reson for this failure

⊙ بنمشي logical ونشوف المشكلة في الـ item نفسها ولا في الـ items اللي هي بتاخد منهم ولا المشكلة في التواصل والتوصيلات بينهم



Safety analysis report

- ⊙ State the events & the required safety mechanism for each.

⑤⑥ develop function safety at S.w & H.w level in parallel.

* The functional Safety requirements of product at Hardware level → steps:
  1. specification.
  2. Design.
  3. implementation.
  4. integration.
  5. Validation.

ممكن نستنتج منها الـ requirements الي هتطبقه على الـ H.w وهيتم تطبيقه الـ concept بتاع الـ Safety
وكمان بعد متعمل الـ safety analysis هتطلع مجموعة الـ requrs الخاصة بالـ H.w

* To make Safety analysis on H.w level use FMEDA

B FMEDA: failure mode effects and diagnostic analysis:

- Automotive ECU consists of diffrent H.w components (resistors, transistors, ---) & ∵ they are H.w then they can fail any time randomly, there we need mechanism to reduce the probability to reduce that from happen, so use (FMEDA).

- Output of FMEDA - Result of analysis [hardware analysis]
  1. Single point fault:
  انه ممكن يكون الـ mechanism المستخدم في الـ Safety مش مغطي كل الجوانب بتاعة الـ item وبالتالي مش هنوصل للـ Safety goals الرئيسية لأن الـ fault مش متغطي بالـ mechanism
  2. probabilistic metric contain residual fault:
  ممكن يكون في fault جزئي ويكون مش كامل بس بيؤدي إلى الـ goal والـ safety مش بتحقق لأن الـ mechanism الي مستخدمينه مش بيمنع الـ fault دا
  3. Latent fault:
  There is fault but I can't know where or what is the reason?

FMEDA Steps

① Collect all the input documents [any document related to H.w]

- H.w circuit
- Top level Safety requirements
- Technical Safety Concept
- operating Conditions

② Calculate the failure rate of each hardware element

نبدأ ندرس كل element في ال H.W .. العمر الإفتراضي ليه و كل حاجة عنه

③ Assign failure mode to each H.w element

يعني .. نمر على كل عنصر H.W و نشوف لو حصله fail إيه اللي هيحصل
في ال item .. وإيه السيناريوهات اللي ممكن يـ fail فيها

④ Apply diagnostic Coverage

نبتدي نعمل فحص لنسبة العطل الموجودة في ال element والتي تم إكتشافها
بواسطة ال safety mech. اللي حطوها

⑤ Make calculations
- → Single point Failure
- → Probabilistic metric contain residual fault.
- → latent fault.

* Product development at S.w level from architecture → to verification of safety requirements

← وال requirements الي بنحددها أو بنتأكد من وجودها وتطبيقها بتتقسم الS.w Safety requirements.

← لو مثلاً عملنا software عنده في بعض ال requirements لازم ناخد بالنا منها وإحنا شغالين طبيعي: require خاصة بال safety وكمان لازم نراعي اننا نغطي الrequirements دي واحنا بنعمل verification من خلال ال ASIL العام بيها.

← يعني لما نعمل Component واخدة ASIL D لازم نعمل testing أكتر علشان نتأكد من وجود كل ال requirements اللي المفروض نتحط فيه.

→ the last 2 points to sure of implement safe S.w.

→ Avoid making code include multiple entry & exit functions.

EX: goto statement

or on embedded level avoid [interrupt Saturation].

---

* To make safety analysis use FMEA on S.w level

FMEA : Falure mode & effect analysis.

→ This approach follow (bottom-up) method unlike (FTA), That mean start from the failure not from the event.

Steps of FMEA

① State possible failures

إيه اللي ممكن يحصل من أعطال؟

② Identify the failure mode effect

إيه تأثير كل failure من اللي أنا توقعتهم؟

③ Assign ASIL level

ال failure دا ممكن يكون sever لأي حد؟

④ implement safety mechanism to avoid falure.

إيه ال mechanism اللي ممكن أعملها علشان أمنع ال failure طبقاً لل ASIL level علشان منوصلش لل safety goal بتاع ال item

EX - if there Component (A) Calculate's the speed
- what if the Calculation is Failed now the output signal is wrong
- The mistaken Calculation used to Control ~~the~~ cur speed.
- That will make vehicle work in wrong speed. ,that will Violate the Safety goal. that been set in the Concept phase.
- needed mechanism:
  - Check on the output signal of the Component if it is true or not.

(7) Safety Validation:

* according to part(4) ... we have to make sure from Safety Validation.
* Follow the steps of part (4) to find out needed requirements. on the system level

(8) Function Safety assessment: تقييم

إتأكد إنه كل الـ Functional safety activities تبعًا و بنفس ترتيب وخطوات الـ Safety life cycle و الـ Plan المناسبة ولازم يكون في document لكل حاجة وبكل خطوة

(9) Production:

(10) operation & services:

iso 26262-2018

* Part 11: added for (Semiconductor product)
  this part gives us overview on the functional safety related to development of Semiconductors.

* Part 12: developed for (motor cycles)
  - now in this edition not only vehicle but all types of other automotive.