Introduction to System Dependability

Kevin Delmas (kevin.delmas@onera.fr)

15 octobre 2021

Lecture overview

Goals provide background to understand how are build dependable systems

- Concepts of dependable systems
- Process used to achieve dependable system
- Dependability Assessment techniques

Plan

- Dependability concepts and process (KD)
- Fault tree analysis (KD) and lab (KD + TP)
- DAL allocation (KD)
- Model based safety assessment (TP) and lab (KD + TP)

Out of lecture scope Operate / maintain system safely

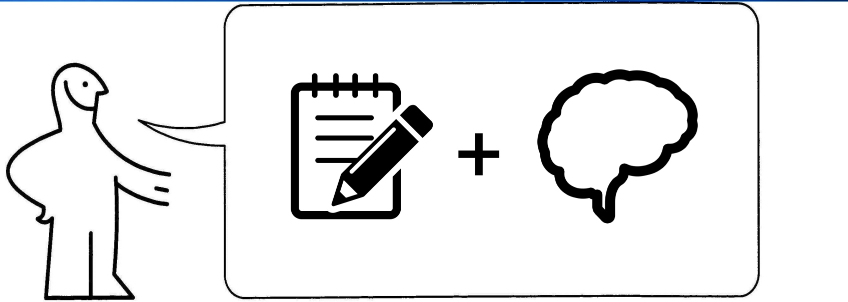
Some definitions are mandatory to understand labs (what a surprise)

= slides preparing computer lab

= reminder (should be)

Be careful !

Interactive course ahead



Numerous exercises during class

Connect to `https://www.sli.do` with 76847

Introduction to System Dependability

What is a system ?

What is a system ?

System

A system is a set of interacting items, forming an integrated whole

System

examples of various complexity : air traffic control, aircraft + pilot, flight-control system, computers, sensors, actuators,...

An example of system

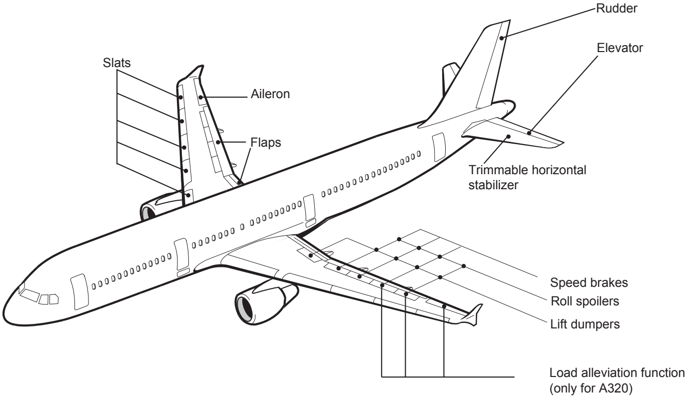


FIGURE – Aircraft actuators

An example of system

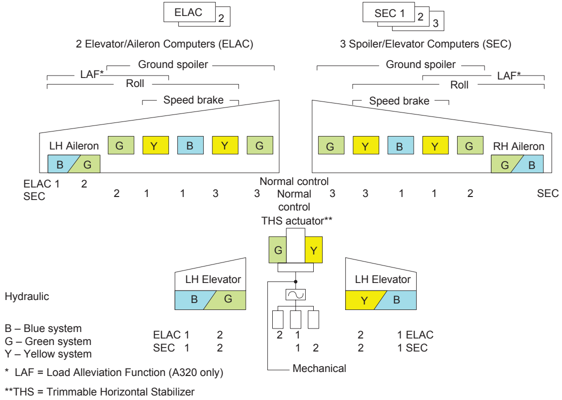


FIGURE – Hydraulic allocation

An example of system : Hydraulic system

Hydraulic power generation and distribution system made of three sub-systems Green, Yellow and Blue.

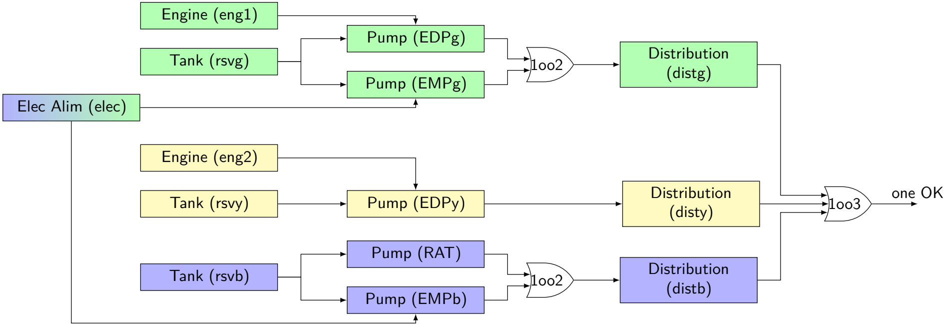


FIGURE – Hydraulic system

An example of system : Pitot sensor

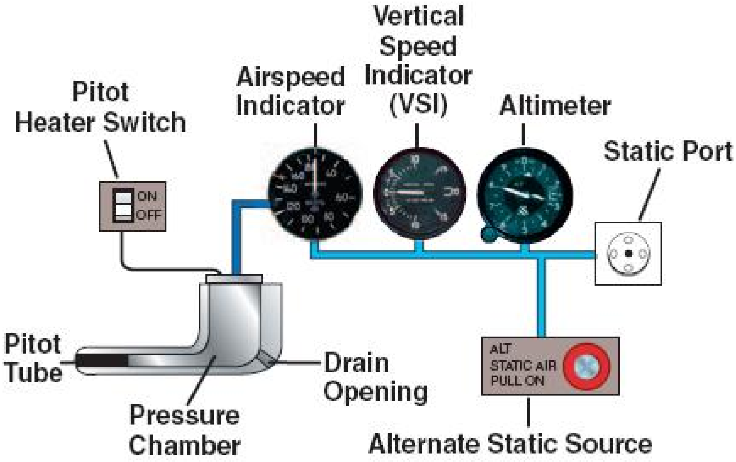
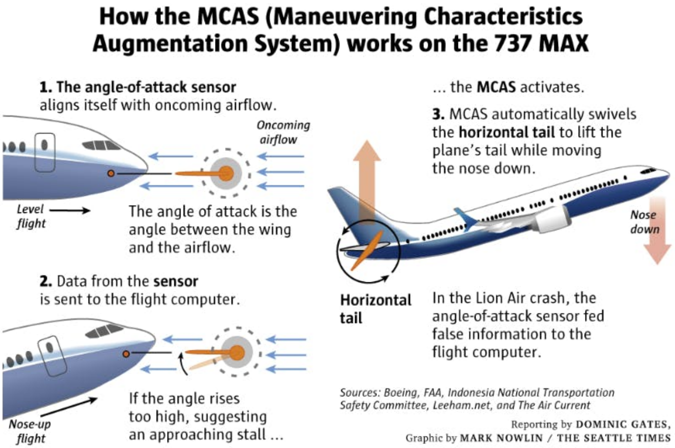


FIGURE – Pitot Static System

An example of system : MCAS



Introduction to System Dependability

What is dependability ?

What is dependability ?

Dependability [ALRL04]

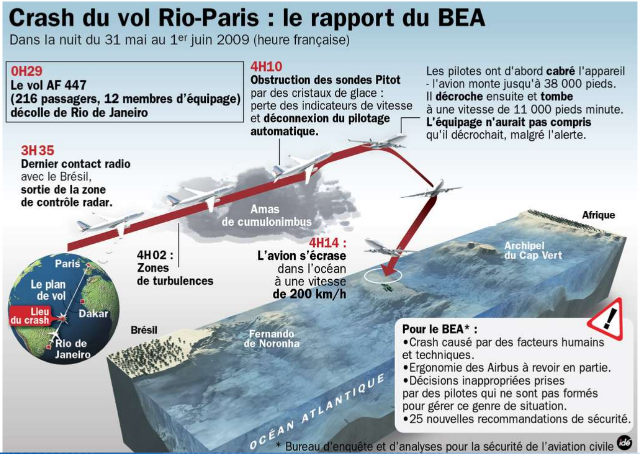
The ability of the system to deliver service that can justifiably be trusted.

Framework to complete the specification beyond the strict definition of what would be expected in a flawless world

- Service specification (and its development and validation)
- Dependability specification (and its development and validation)

Consequences of flaws : Pitot icing

BEA accident report available here



Consequences of flaws : erroneous MCAS activation

KNKT accident report available here

Resumed Flight History :

- Unintended trigger of the MCAS (assumed cause erroenous AOA sensor)
- Crew was not able to identify cause of MCAS activation and tried multiple manual overrides
- Crew considered (unusual) that situation not require a landing to nearest airport
- Eventually, final MCAS accivation leads to descente rate above 10000 feet/min

Need to identify and handle the dependability threats

Dependability concepts

Dependability threats (what can go wrong) :

failure occurrence of the deviation of the delivered service from expectations

- severity : harm of its direct or indirect consequences
- mode : characterization of the way a system/item fails
- consistency : Byzantine failure
- rate : probability of failure per unit of time of items in operation

error Part of the state of the system which may lead to a failure

- latent or detected

fault hypothesized or adjudged cause of an error state

- Dormant or active, internal or external (w.r.t. system boundaries)
- Physical or human (accidental or intentional), in development or operation
- Temporary (transient, intermittent), permanent

Recursive propagation path :

$$\text{fault} \Rightarrow \text{error} \Rightarrow \text{failure} \Rightarrow \ldots$$

Hydraulic system

Nominal function hydraulic power delivery

Failure no delivery of hydraulic power

Failure modes

- total loss of delivery of hydraulic power (loss of the three lines)
- partial loss of delivery of hydraulic power (loss of one line)

Behavior under fault

System/items behaviors depend on

- control/observation interface
- internal states (not always distinguishable)
  - nominal functioning modes
  - error states part of the total state of a system/item that may lead to its subsequent failure

Hydraulic system

Failure mode loss of delivery of hydraulic power on one pipe on demand

Error state hydraulic pipe broken

Fault

- Primary (intrinsic) cause : pipe wearing
- Secondary cause (extrinsic) : pipe received too high pressure fluid

Observability Not detectable when not power is demanded (pump off)

Concretely, how to evaluate dependability ?

Dependability attributes

Dependability assessed using a set of quantitative and qualitative attributes such as :

- **Availability** Readiness of the service
- **Reliability** Continuity of the service
- **Maintainability** Ability to undergo repair
- **Safety** ability to avoid too severe consequences (human, environment)
- **Security** ability to ensure condfidentiality (non disclosure to unauthorized users), integrity (malicious alterations) and availability (no DoS) of the service

Math corner : Availability

Availability(A)

Ability of a system S to deliver a correct service at a given time :

$$A(t) = p(S \text{ non faulty at } t)$$

Availability

In the space domain :

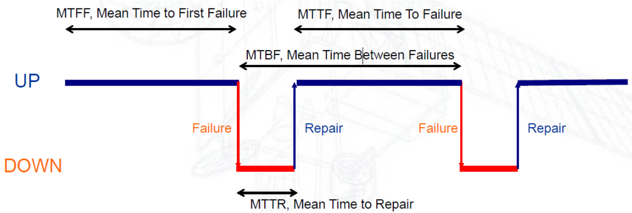
- Launcher : capability to launch at the scheduled time
- Satellite : capability to perform some critical mission phases (*e.g.* orbit insertion, fly-by)

Math corner : Availability

Average availability

Proportion of up-time between 0 and t (or over the lifetime)

$$A = MTTF/MTBF$$



Math corner : Reliability

Reliability(R)

Ability of a system S to ensure continuity of correct service :

$$R(t) = p(S \text{ non faulty over } [0, t])$$

Reliability

In the space domain :

- Launcher : reliability characterises the mission success
- Satellite : reliability characterises the lifetime through the probability to have not experienced any fatal failure at t

Math corner : Safety

Safety

Ability of a system S to avoid harmful events (human, environement)

Safety

In the space domain :

- Launcher : explosion, fall-down of large pieces or toxic material
- Satellite :
  - ground operations,
  - in-orbit servicing, docking (e.g., ATV with the International Space Station),
  - end of life, re-entry

Math corner : Failure rate & Maintainability

Maintainability(M)

Ability of a system S to undergo modifications and repair

$$M(t) = 1 - p(S \text{ non repaired over } [0,t])$$

Failure Rate (Λ)

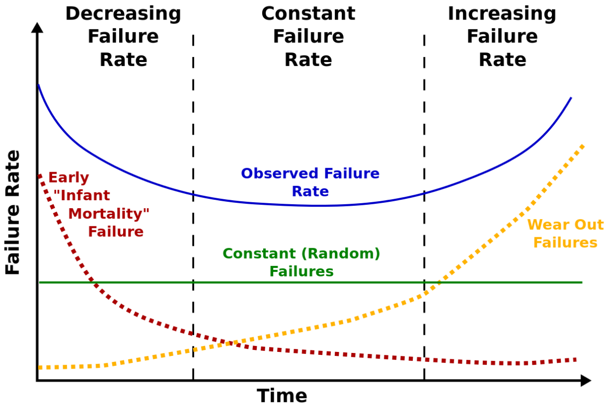
Probability of a system S to fail at $t + dt$ knowing it has not failed over $[0,t]$:

$$\Lambda(t) = \lim_{dt \to 0} \frac{p(S \text{ fails during } [t, t+dt])}{dt} \frac{1}{R(t)}$$

Relation with R :

$$R(t) = e^{-\int_0^t \Lambda(u)du}$$

Math corner : Bath curve failure rate



Assume items used during constant failure rate phase

Math corner : Computation approximation

Rare failure assumptions

When $\lambda t \sim 0$ (usually $\lambda t < .1$) use Taylor expansion for computations :

$$\overline{R}(t) = 1 - R(t) = 1 - e^{-\lambda t} \underset{0}{\sim} \lambda t$$

Independence & pessimism assumption

If two components C_1 and C_2 have independent failures with failure rate λ_1 and λ_2

$$\begin{aligned}
p(\text{both fail}) &\underset{\text{independent}}{=} p(C_1 \text{ fails})\, p(C_2 \text{ fails}) = \lambda_1 \lambda_2 t^2 \\
p(\text{one fails}) &= p(C_1 \text{ fails}) + p(C_2 \text{ fails}) - p(\text{both fail}) \\
&\underset{\text{pessimism}}{=} p(C_1 \text{ fails}) + p(C_2 \text{ fails})
\end{aligned}$$

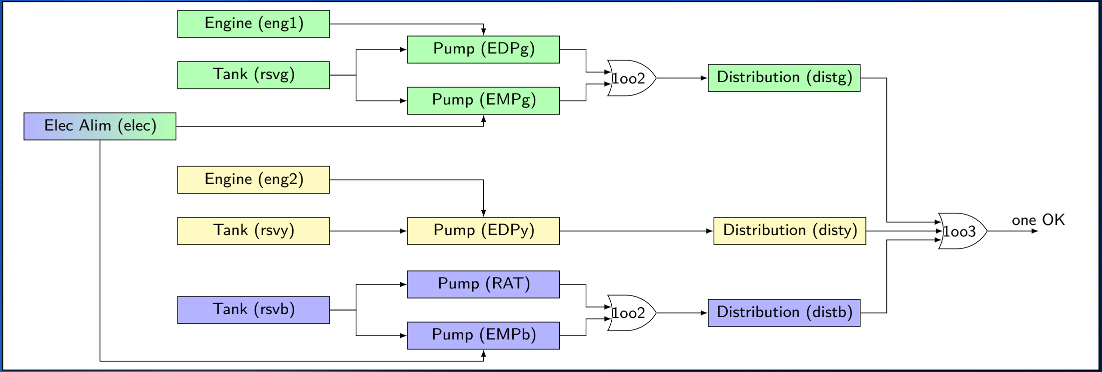
How to ensure dependability ?

Dependability means

Faults leading to harmful events can be :

- **Prevented** Avoid to introduce fault during the design of the system *e.g.* correct by construction design, rigourous development process
- **Tolerated** Deal with the possible errors and failures caused by residual faults *e.g.* architectural tolerance, defensive programming
- **Removed** Track and remove faults introduced during the system design *e.g.* formal code verification, specification-oriented test
- **Forecasted** Predict the time of the next fault and apply preventive actions to avoid subsequent errors *e.g.* predictive maintenance

Can you identify a dependability means used to handle failures in the hydraulic system ?



Fault tolerance by structural redundancy

Strategy Implement various element capable of delivering a given (critical) service

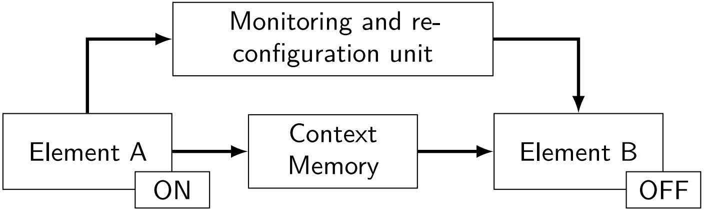
Selective Redundancy Provide service out of two elements

- Hot redundancy if both are active
- Warm/Cold redundancy if one of the component is used as a backup

N-modular redundancy Duplex, majority voting

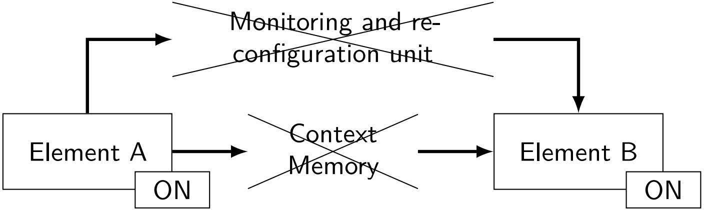
Useful only if indenpendency w.r.t to faults *i.e.* ensure diversification during design

Cold Redundancy



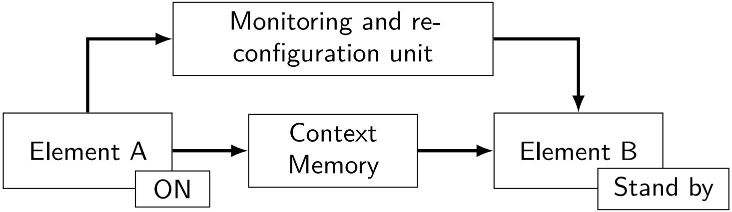
- Most often used for space systems
- Most reliable as the failure rate of an unpowered element is generally significantly lower than of a powered one (about one tenth)

Hot Redundancy



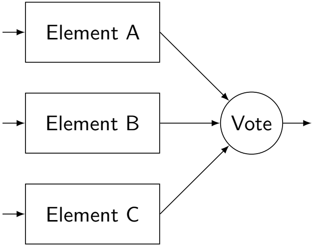
- Need to define output selection process
- Lower long-term reliability
- Useful if the backup cannot be activated in case of failure (*e.g* telecommunication)
- Useful if equipment for which no interruption of service is tolerated (*e.g.* launcher flight control)

Warm Redundancy



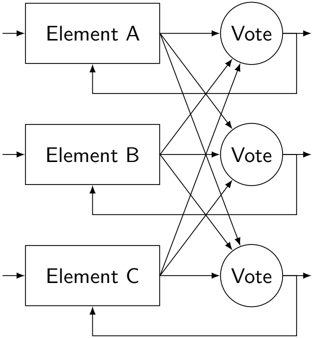
- For equipment with a long start-up time (*e.g.* computers)
- Ensure very short reconfiguration times
- More complex to manage (periodic backup and upload of context, alarm watchdog & reconfiguration)

N-Modular redundancy



- Ensure service continuity in case of single failure on elements
- Caution, voter can be considered as single point of failure
- Common case/mode faults on elements

N-Modular N-Voting redundancy



- Ensure service continuity in case of single failure on elements
- Possible element deactivation after desagreement
- Common case/mode faults on elements

Example of self checking components

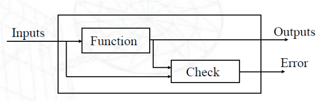


FIGURE – Fail-stop block

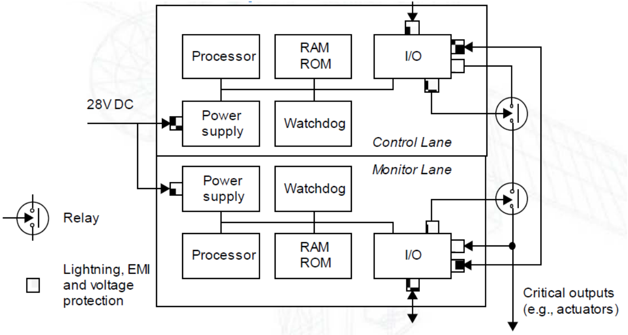


FIGURE – Airbus Command/Monitor (COM/MON) computers

Combining fault tolerance mechanisms

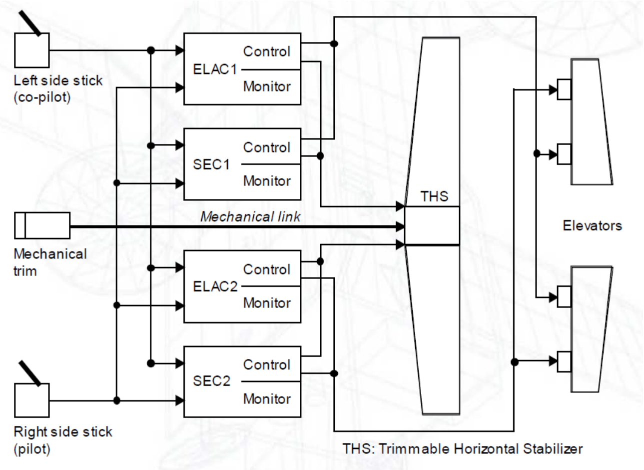


FIGURE – Aircraft fly-by-wire

OK, but would you take a plane if $1 - R_{\text{total loss}}(10^3 h) = 10^{-4},\ 10^{-6}$?

OK, but would you take a plane if $1 - R_{\text{total loss}}(10^3 h) = 10^{-4},\ 10^{-6}$?

It depends . . .

Risk acceptability

The question is :

What happens if ?

Risk acceptability

The question is :

What happens if hydraulic system fails ?

Risk acceptability

The question is :

What happens if hydraulic system fails ?

- No power in actuators
- Loss of trajectory control
- Depending on flight phase, injury or death of passengers and/or aircraft crew.

Risk acceptability

New question :

Knowing the severity of the failure, what is an acceptable frequency of such failure ?

Another general definition of dependability :

"ability to avoid service failures that are frequent and more severe than acceptable"

What does service failure, severe, frequent, acceptable mean ?
⇒ Regulatory texts

Regulatory texts & norms

Regulation For safety-critical systems, regulation are provided as regulatory texts such as :

- Safe use of nuclear technology for peaceful applications, IAEA, 1957
- Peaceful use of outer space, COPUOS, 1958
- Certification specification for large aeroplanes, EASA, 2003
- Certification specification for large rotorcraft, EASA, 2003

Norms & Standards Acceptable means of compliance to the regulatory texts
$\Rightarrow$ sometimes applied by applicant without existing regulation (*e.g.* automotive)

Overview of standards by domain

Aeronautics
- System related : ARP4761, APR4754-A
- Hardware related : DO254
- Software related :DO178-C

Automotive ISO26262

Nuclear IEC 60880, IAEA DS-431

Railway EN 50128, 50126, 50129, 50155, IEC 61508

Space ECSS

Qualification vs Certification

Qualification Activities granting a confidence level to an entity (person, organisation or artefact)
$\Rightarrow$ Activities tailored to the context of qualification : item, actors, usage, timeline

Certification An assessment body substantiates to an Authority that the engineering process of an applicant ensures regulatory safety objectives through conformance to safety standards

Actors per domain

Domain	Applicant	Regulation	Autority	Assessment Body
Aeronautics	Manufacturer	Yes	EASA-FAA	EASA-FAA
Automotive	Manufacturer	No	No	No
Nuclear	Operator	Yes	National agency (*e.g.* ASN)	ASN, IRSN (France)
Railway	Manufacturer	Yes	ERA	CERTIFIER, ...
Space	Manufacturer	Yes	National agency	CNES (France), NASA/FAA (USA)

Integration of the safety

Safety mechanisms can be designed as :

- A dedicated system monitoring and piloting the actual system
  - possible when high-level emergency actions (*e.g.* core shutdown) ensure to reach a safe state
  - classically used in railway and nuclear domains
- A set of component integrated in the system itself
  - mandatory when service interruption is harmful (*e.g.* flight controller)
  - classically used in aeronautics
- A combination of the two (spatial and automotive domain)

Demonstration of the safety : Means vs objectives

Norms and standard can demonstrate compliance to regulation by :

- Providing high-level objectives (aeronautics, nuclear, space)
  - ⊕ (Quite) Generic and applicable to various context
  - ⊖ Applicant need to provide a compelling demonstration of the compliance to the objective
- Providing specific means and activities (railway, automotive)
  - ⊕ Simplify verification of the compliance
  - ⊖ Tailored to a specific context, need updates for each new technology, system, tools

Demonstration of the safety : Common philosophy

Across all the applicative domains use the notion of criticality/assurance/integrity level

Levels are used to :

- tailor requested objectives and activities
  ⇒ risk-driven effort
- identify and avoid failure propagation from "low cofidence" elements (*e.g.* passenger entertainment system) to "high confidence" elements (*e.g.* flight management system)

How these concepts are implemented for large civil aircraft ?

Risk acceptability for civil aircraft

When considering safety of civil aircraft :

Failure Condition (FC) kind of service failures that :

- has an effect on the aircraft and its occupants, both direct and consequential,
- caused by one or more failures, considering relevant adverse operational or environmental conditions.

Severity Failure Condition is classified in accordance to the severity of its effects as defined .

Risk acceptability for civil aircraft

severity class	effects description	acceptable frequency
catastrophic	prevent continuous safe flight and landing : aircraft loss and loss of crew and passengers	$< 10^{-9}$ per flight hour and no single failure leads to the FC
hazardous	large reduction in safety margins or functional capabilities or physical distress or high crew workload or serious or fatal injuries to a relatively small number of passengers	$< 10^{-7}$ per flight hour

Risk acceptability for civil aircraft

severity class	effects description	acceptable frequency
major	significant reduction in safety margin or functional capabilities or significant increase in crew workload or discomfort to occupants possibly including injuries	$< 10^{-5}$ per flight hour
minor	no significant reduction in aircraft safety.	$< 10^{-3}$ per flight hour
no safety effect		

Risk acceptability for civil aircraft

Severity & objectives

"Total loss of hydraulic system " is classified , so

Risk acceptability for civil aircraft

Severity & objectives

"Total loss of hydraulic system " is classified Catastrophic, so

- the probability rate of this failure condition shall be less than 10^{-9} /FH and
- No single event shall lead to this failure condition

Warnings :

- The regulation is not the same for military aircraft
- The regulation for civil UAV is still in discussion
- A generic agreed classification is an open question for a lot of domains

How to apply these concepts to build a complex dependable system ?

Process based approach

Main steps :

- Identify dependability requirements
- Specify a system architecture to ensure these properties
- Assess whether the proposed specification fulfills the dependability requirement
- If OK, refine the system design and iterate

Guidelines tuned according to the system kind :

- ISO 26262 [ISO10] for automotive systems
- ECSS Q-ST 40 for space systems
- ARP 4754A [SAE10], ARP 4761 [SAE96] for aeronautic systems

Dependability & development process

Integrated dependability process in development process ⇒ Avoid late detection of dependability issues

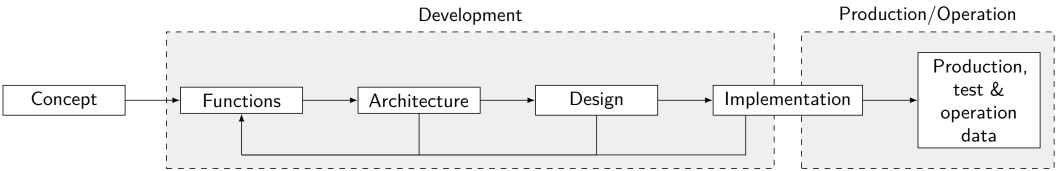


FIGURE – Development life cycle

When should we perform safety activities ?

Dependability & development process

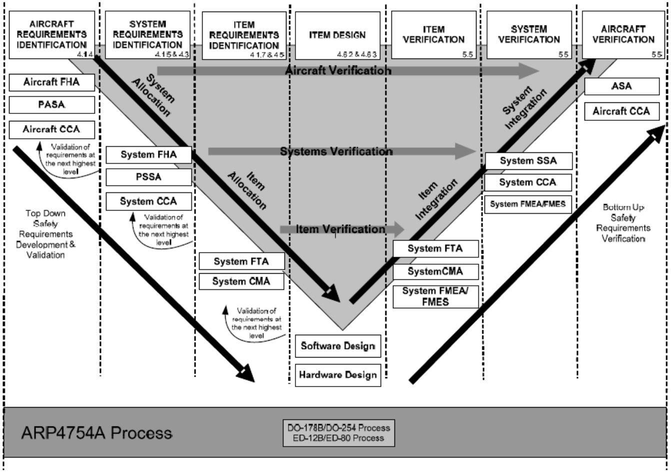
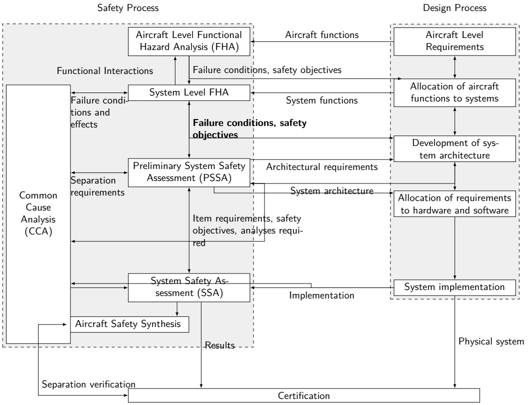


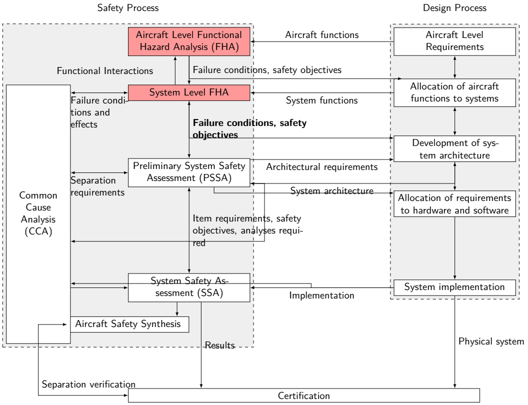
FIGURE 5 - INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

Safety Process (Complete)



When should we identify and classify Failure Conditions ?

Safety Process (FHA)



Functional Hazard Assessment (FHA)

Definition Systematic, comprehensive examination of functions to identify and classify FCs of those functions according to their severity

Process

1. identify functions associated with the system under study
2. identify and describe FCs associated with these functions, considering single and multiple failures in normal and degraded environments
3. determine effects of the FC
4. classify FC effects on the aircraft (cat, haz, maj, min, no safety effect)

Simplified FHA by the example

System	Function	Failure Mode	Context	Effects	Criticality
Hydraulic system	Generate hydraulic power	Total loss	During cruise		

Table – Simplified FHA of Hydraulic system

Simplified FHA by the example

System	Function	Failure Mode	Context	Effects	Criticality
Hydraulic system	Generate hydraulic power	Total loss	During cruise	Loss of aircraft controllability	

Table – Simplified FHA of Hydraulic system

Simplified FHA by the example

System	Function	Failure Mode	Context	Effects	Criticality
Hydraulic system	Generate hydraulic power	Total loss	During cruise Annunciated during taxi	Loss of aircraft controllability	Catastrophic

Table – Simplified FHA of Hydraulic system

Simplified FHA by the example

System	Function	Failure Mode	Context	Effects	Criticality
Hydraulic system	Generate hydraulic power	Total loss	During cruise	Loss of aircraft controllability	Catastrophic
			Annunciated during taxi	Evacuation of passengers	Minor
		Partial loss	During cruise		

Table – Simplified FHA of Hydraulic system

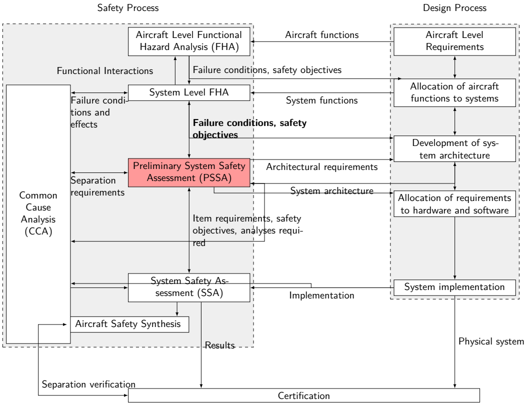
Simplified FHA by the example

System	Function	Failure Mode	Context	Effects	Criticality
Hydraulic system	Generate hydraulic power	Total loss	During cruise	Loss of aircraft controllability	Catastrophic
			Annunciated during taxi	Evacuation of passengers	Minor
		Partial loss	During cruise	Limited controllability of aircraft	Minor

TABLE – Simplified FHA of Hydraulic system

When should we check dependability requirements ?

Safety Process (PSSA)



How to check dependability requirements ?

$\Rightarrow$ several complementary methods

Failure Modes and Effects Analysis (FMEA)

Definition Inductive analysis of local and global effects of all components failures

Process Fill-up for each system component following table.

Failure Modes and Effects Analysis (FMEA)								
Aircraft : Function : System : Sub-system : Component :								
No	Item	Function	Failure Mode	Failure Cause	Failure Rate	Failure Effects	Recognition failure	Remarks

Failure Modes and Effects Analysis (FMEA)

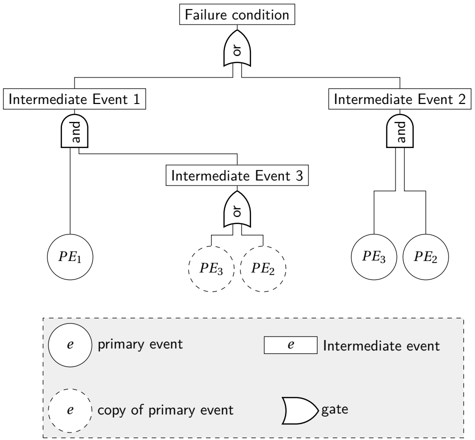
Definition Inductive analysis of local and global effects of all components failures

Process Fill-up for each system component following table.

Failure Modes and Effects Analysis (FMEA)								
Aircraft :		XXX						
Function :		Deceleration on ground						
System :		Hydraulic Power Generation & Distribution						
Sub-system :		Green System						
Component :		Pipe						
No	Item	Function	Failure Mode	Failure Cause	Failure Rate	Failure Effects	Recognition failure	Remarks
1	Green Pipe	Power distribution	Loss	Aging	10^{-4}	Loss of green system, hydraulic system remains available for aircraft	Warning on pilot display	Select "Green pump off" and turn on power transfert unit

What is the link between primary events and failure conditions?

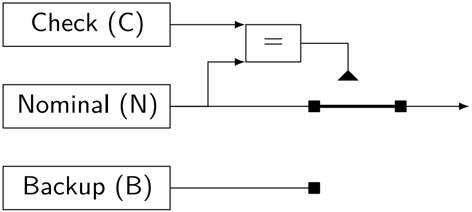
Failure propagation : The Fault Tree



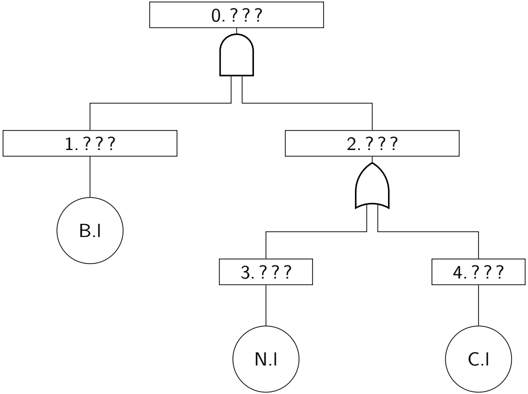
Legend

Failure propagation : The Fault Tree example

Functional View

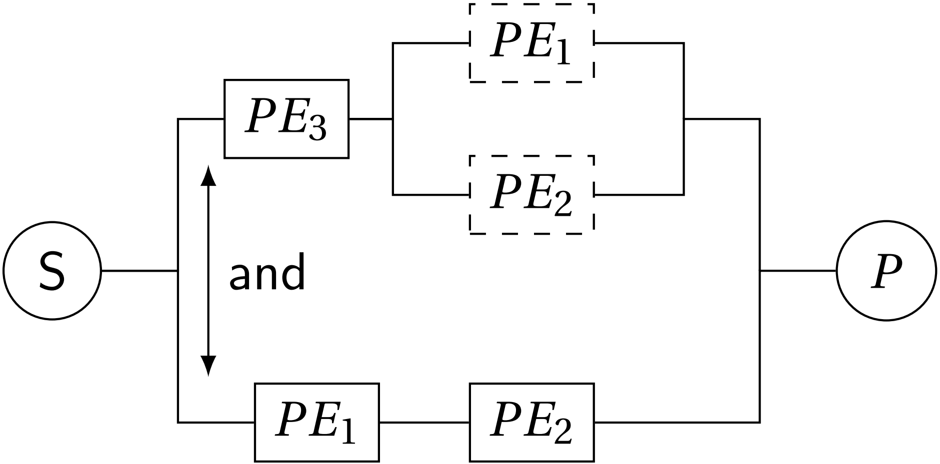


Fault tree



Failure propagation : Reliability Block Diagram

Alternative notation for fault trees (analogy with serial-parallel electrical circuits)



How do we use these representations ?