Requirements verification

⚠ We assume that primary events are independent

1. Determine the failure conditions and their criticality (from FHA)
2. Build the fault trees for each failure condition
3. Compute the minimal cutsets
4. Qualitative verification : Compute the order and compare it to the required bound
5. Quantitative verification : Compute the probability and compare it to the required bound

What if some primary events are not independent (tire burst, engine burst,...) ?

Deal with dependencies

What could cause the simultaneous failure of several components ?

- Adversary conditions : overheat, electromagnetic perturbations, ...
- Destruction of a whole zone : engine burst, in-flight fire,...
- But also : implementation common mode (functions depending on the same equipments), specification errors, systematic development errors,...

What are the consequences ?

- Possible violation of safety objective
  $\Rightarrow$ Identify and analyze common mode during the Common Cause Analysis (CCA)

Deal with dependencies

Example (Dependencies impact)

Minimal cut $C = \{a, b\}$ for a catastrophic FC, if a and b are not independent (triggered by d) :

$\Rightarrow$ $C \rightarrow \{d\}$

$\Rightarrow$ Order goes from 2 to 1

⚠ System does not fulfil requirements

Deal with dependencies

Event in MCS shall be independent to avoid that their implementation introduces a common mode reducing the size of the MCS under the order requirement.

$$\Downarrow$$

Define the segregation requirements to ensure independence

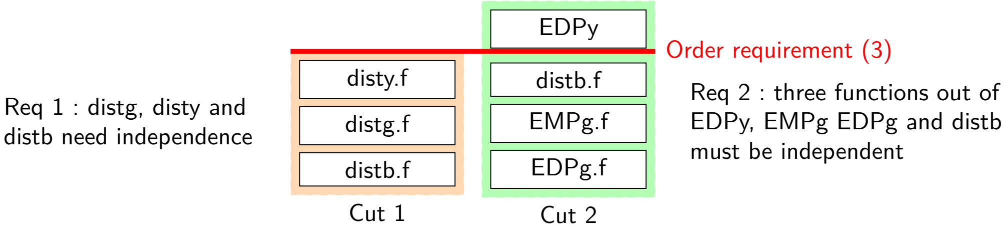


Figure – Independence requirements for Total hydraulic system loss

Deal with dependencies

1. Define the independence groups :
   - Two members of the same group are not independent
   - Two members of different groups are independent

Example (Independence groups)

Let consider that component can be in three spacial zones, each zone can be completely destroyed by an engine burst, the independent groups are :

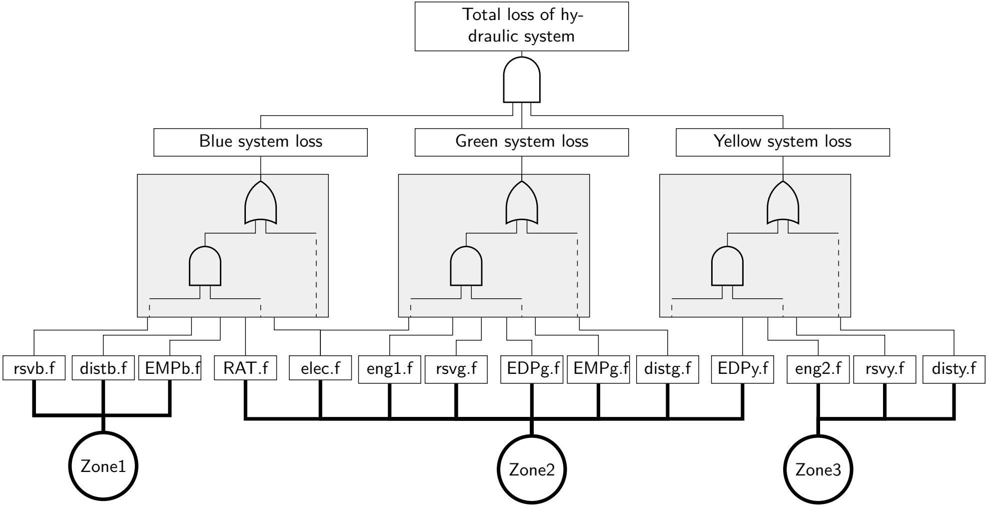
Zone 1	Zone 2	Zone 3
rsvb, distb, EMPb	RAT, elec, eng1, rsvg, EDPg, EMPg, distg, EDPy	rsvy, eng2, disty

Deal with dependencies

1. Define the independence groups :
   - Two members of the same group are not independent
   - Two members of different groups are independent
2. Modify the fault tree :
   - transform primary event as intermediate events
   - create a primary event per group
   - link intermediate event to the corresponding group
3. Compute the cutsets
4. Check the requirements

Considering the previous independence groups, is the system safe ?

Deal with dependencies : Example



Deal with dependencies : Example

$$
\begin{array}{cccc}
\{EDPg.f, & RAT.f, & elec.f, & EDPy.f\} \\
\Downarrow & \Downarrow & \Downarrow & \Downarrow \\
\{Zone2, & Zone2, & Zone2, & Zone2\} \\
\end{array}
$$

$$\Downarrow Minimisation$$

$$\{Zone2\}$$

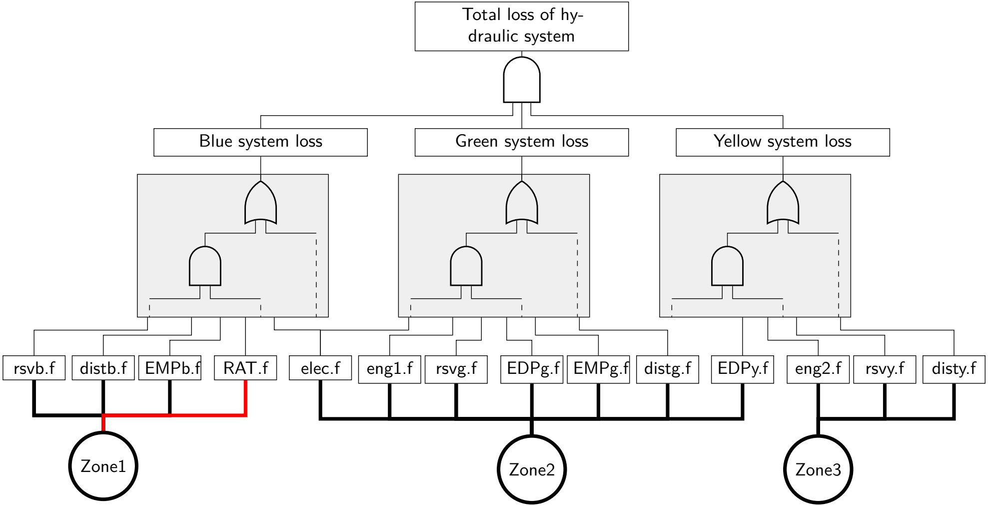
$$\Downarrow$$

Order is 1

$$\Downarrow$$

KO since "Total loss of hydraulic system" is Catastrophic so requirement is 2

Deal with dependencies : Example



Deal with dependencies : Example

$$\{\{EDPg.f,\ RAT.f,\ elec.f,\ EDPy.f\},\cdots\}$$
$$\Downarrow Analysis$$
$$\{\{Zone1,\ Zone2\}\}$$

$$\Downarrow$$

Order is 2

$$\Downarrow$$

OK since "Total loss of hydraulic system" is Catastrophic so requirement is 2

Minimal cutsets computation

What could cause the simultaneous failure of several components ?

- Adversary conditions : overheat, electromagnetic perturbations, ...
- Destruction of a whole zone : engine burst, in-flight fire,...
- But also : implementation common mode (functions depending on the same equipments), specification errors, systematic development errors,...

Minimal cutsets computation

What could cause the simultaneous failure of several components ?

- Adversary conditions : overheat, electromagnetic perturbations, . . . ⇒ Random faults
- Destruction of a whole zone : engine burst, in-flight fire,. . . ⇒ Random faults
- But also : implementation common mode (functions depending on the same equipments), specification errors, systematic development errors,. . . ⇒ Systematic faults

Acceptability cannot be based on probability assessment !
⇒ ensure a level of confidence in development correctness

Minimal cutsets computation

DAL Development Assurance Level (ARP4754) is the level (from E to A) of rigor of development assurance tasks performed on functions and items (software, hardware) whose fault result

Warning :

- DAL can be associated with
  - Functions : FDAL
  - Items : IDAL
- For each DAL level, assurance activities are listed in :
  - ARP4754 for FDAL
  - DO178 (SW) and DO254 (HW) for IDAL

Assurance Activities Examples

	Objective		Applicability			
	Description	Ref	A	B	C	D
1	Software high-level requirements comply with system requirements.	6.3.1a	I	I	R	R
2	High-level requirements are accurate and consistent.	6.3.1b	I	I	R	R
3	High-level requirements are compatible with target computer.	6.3.1c	R	R		

- High DAL level ⇒ great number of assurance activities
  ⇒ costly
  ⇒ minimize the DAL of software and hardware

DAL Allocation : Basic Allocation

Based on the severities of the FCs that function fault contributes to.

Sev(FC)	DAL(FC)
CAT	A
HAZ	B
MAJ	C
MIN	D
NSE	E

TABLE – Link between severity and DAL

What does "the severities of the FCs that function fault f contributes to" mean ?

$\Rightarrow$ the severities of the FCs whose MCS contains f

DAL Allocation : Basic Allocation

Context
- Let fc_1 (resp fc_2) be a failure condition of severity HAZ (resp. MAJ)
- Let $MCS_1 = \{\{f_1, f_2, f_4\}, \{f_3\}\}$ and $MCS_2 = \{\{f_1, f_3\}\}$

Question What is the basic DAL of f_1 ?

DAL Allocation : Basic Allocation

Context
- Let fc_1 (resp fc_2) be a failure condition of severity HAZ (resp. MAJ)
- Let $MCS_1 = \{\{f_1, f_2, f_4\}, \{f_3\}\}$ and $MCS_2 = \{\{f_1, f_3\}\}$

Question What is the basic DAL of f_1 ?

Answer f_1 contained in MCS_1 and MCS_2 so
$DAL(f_1) = worst(DAL(fc_1), DAL(fc_2)) = DAL(HAZ) = B$

Question What is the basic DAL of f_2 ?

DAL Allocation : Basic Allocation

Context
- Let fc_1 (resp fc_2) be a failure condition of severity HAZ (resp. MAJ)
- Let $MCS_1 = \{\{f_1, f_2, f_4\}, \{f_3\}\}$ and $MCS_2 = \{\{f_1, f_3\}\}$

Question What is the basic DAL of f_1 ?

Answer f_1 contained in MCS_1 and MCS_2 so
$DAL(f_1) = worst(DAL(fc_1), DAL(fc_2)) = DAL(HAZ) = B$

Question What is the basic DAL of f_2 ?

Answer f_2 contained only in MCS_1 so $DAL(f_2) = worst(DAL(fc_1)) = DAL(HAZ) = B$

DAL Allocation : Degradation rules

Designer can downgrade the basic DAL $basic$ of a function using independence, the allocation must fulfill the following rules :

Rule 1 $basic$ can be degraded at most by two levels

Rule 2 For all cuts $\{f_1, \cdots, f_n\} \in MCS_{fc}$ where $f_1, \cdots, f_n$ are independent, either :

- Option 1 : it exists f_i such that $DAL(f_i) = basic$
- Option 2 : it exists f_i, f_j such that $DAL(f_i) = DAL(f_j) = basic - 1$

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $=$ 20, DAL B $=$ 15, DAL C $=$ 5, DAL D $=$ 4, DAL E $=$ 0

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ B	$\geq$ D	-	$\geq$ D	1

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $=$ 20, DAL B $=$ 15, DAL C $=$ 5, DAL D $=$ 4, DAL E $=$ 0

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ B	$\geq$ D	-	$\geq$ D	1
	$\{f_3\}$	-	-	$\geq$ B	-	-

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $=$ 20, DAL B $=$ 15, DAL C $=$ 5, DAL D $=$ 4, DAL E $=$ 0

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ B	$\geq$ D	-	$\geq$ D	1
	$\{f_3\}$	-	-	$\geq$ B	-	-
C	$\{f_1, f_3\}$	$\geq$ C	-	$\geq$ E	-	1

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ B	$\geq$ D	-	$\geq$ D	1
	$\{f_3\}$	-	-	$\geq$ B	-	-
C	$\{f_1, f_3\}$	$\geq$ C	-	$\geq$ E	-	1
Result		$\geq$ B	$\geq$ D	$\geq$ B	$\geq$ D	
Cost		38				

Is it the cheapest option ?

$\Rightarrow$ Let's try again !

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2
	$\{f_3\}$	-	-	$\geq$ B	-	-

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2
	$\{f_3\}$	-	-	$\geq$ B	-	-
C	$\{f_1, f_3\}$	$\geq$ E	-	$\geq$ C	-	1

DAL Allocation : Degradation rules

Suppose f_1, f_2, f_3 and f_4 are independent and cost : DAL A $= 20$, DAL B $= 15$, DAL C $= 5$, DAL D $= 4$, DAL E $= 0$

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_1, f_2, f_4\}$	≥ C	≥ C	-	≥ D	2
	$\{f_3\}$	-	-	≥ B	-	-
C	$\{f_1, f_3\}$	≥ E	-	≥ C	-	1
Result		≥ C	≥ C	≥ B	≥ D	
Cost		29				

Whoopsie, f_1 and f_3 are not independent

$\Rightarrow$ Any impact on last allocation ?

DAL Allocation : Degradation rules

f_1, f_3 not independent $\Rightarrow$ replace them by a new function failure $f_{1,3}$.

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	

DAL Allocation : Degradation rules

f_1, f_3 not independent $\Rightarrow$ replace them by a new function failure $f_{1,3}$.

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_{1,3}, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2

DAL Allocation : Degradation rules

f_1, f_3 not independent $\Rightarrow$ replace them by a new function failure $f_{1,3}$.

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_{1,3}, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2
	$\{f_{1,3}\}$	-	-	$\geq$ B	-	-

DAL Allocation : Degradation rules

f_1, f_3 not independent $\Rightarrow$ replace them by a new function failure $f_{1,3}$.

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_{1,3}, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2
	$\{f_{1,3}\}$	-	-	$\geq$ B	-	-
C	$\{f_{1,3}\}$	$\geq$ C	-	$\geq$ C	-	-

DAL Allocation : Degradation rules

f_1, f_3 not independent $\Rightarrow$ replace them by a new function failure $f_{1,3}$.

basic DAL	cuts	DAL				Option
		f_1	f_2	f_3	f_4	
B	$\{f_{1,3}, f_2, f_4\}$	$\geq$ C	$\geq$ C	-	$\geq$ D	2
	$\{f_{1,3}\}$	-	-	$\geq$ B	-	-
C	$\{f_{1,3}\}$	$\geq$ C	-	$\geq$ C	-	-
Result		$\geq$ C	$\geq$ C	$\geq$ B	$\geq$ D	
Cost		29				

Your turn ! Allocate the DAL of green system

DAL Allocation : Exercise

Assume FC is Major, all independent except EMP and $eng1$, and DAL cost for EDP and $elec$ is twice the initial cost.

basic DAL	cuts	DAL						Option
		$dist$	rsv	EMP	EDP	$eng1$	$elec$	
?	$\{dist\}$	$\geq ?$	-	-	-	-	-	?
	$\{rsv\}$	-	$\geq ?$	-	-	-	-	?
	$\{EMP, EDP\}$	-	-	$\geq ?$	$\geq ?$	-	-	?
	$\{EMP, eng1\}$	-	-	$\geq ?$	-	$\geq ?$	-	?
	$\{elec, EDP\}$	-	-	-	$\geq ?$	-	$\geq ?$	?
	$\{elec, eng1\}$	-	-	-	-	$\geq ?$	$\geq ?$	?
Result		$\geq ?$	$\geq ?$	$\geq ?$	$\geq ?$	$\geq ?$	$\geq ?$	
Cost		?						

DAL Allocation : Exercise

Assume FC is Major, all independent except EMP and $eng1$, and DAL cost for EDP and $elec$ is twice the initial cost.

basic DAL	cuts	DAL						Option
		$dist$	rsv	EMP	EDP	$eng1$	$elec$	
C	$\{dist\}$	$\geq$ C	-	-	-	-	-	-
	$\{rsv\}$	-	$\geq$ C	-	-	-	-	-
	$\{f_{EMP,eng1}, EDP\}$	-	-	$\geq$ C	$\geq$ E	-	-	1
	$\{f_{EMP,eng1}\}$	-	-	$\geq$ C	-	$\geq$ C	-	-
	$\{elec, EDP\}$	-	-	-	$\geq$ D	-	$\geq$ D	2
	$\{elec, f_{EMP,eng1}\}$	-	-	-	-	$\geq$ C	$\geq$ E	1
Result		$\geq$ C	$\geq$ C	$\geq$ C	$\geq$ D	$\geq$ C	$\geq$ D	
Cost		36						

What about IDAL ?

DAL Allocation : IDAL

- IDAL is derivated from the FDAL of the functions implemented by the item
- Same rules as FDAL but cannot downgrade DAL twice (in function and item)

Why should we avoid double downgrade ?

DAL Allocation : IDAL

- Let FC be a CAT and $MCS_{fc} = \{\{f_1, f_2, f_3\}\}$ where f_i are mutually independent.
- Each f_i needs at least one item $i_i^{f_i}$ and all items are independent.
- What is the IDAL of $i_i^{f_i}$ without no double downgrade rule ?

DAL Allocation : IDAL

- Let FC be a CAT and $MCS_{fc} = \{\{f_1, f_2, f_3\}\}$ where f_i are mutually independent.
- Each f_i needs at least one item $i_i^{f_i}$ and all items are independent.
- What is the IDAL of $i_i^{f_i}$ without no double downgrade rule ?
- Apply option 1 on FDAL $\Rightarrow FDAL(f_1) = B, FDAL(f_2) = B, FDAL(f_3) = C$
- Apply option 1 on IDAL $\Rightarrow IDAL(i_1^{f_1}) = C, IDAL(i_2^{f_1}) = C, \cdots$

DAL Allocation : IDAL

- Let FC be a CAT and $MCS_{fc} = \{\{f_1, f_2, f_3\}\}$ where f_i are mutually independent.
- Each f_i needs at least one item $i_i^{f_i}$ and all items are independent.
- What is the IDAL of $i_i^{f_i}$ without no double downgrade rule ?
- Apply option 1 on FDAL $\Rightarrow FDAL(f_1) = B, FDAL(f_2) = B, FDAL(f_3) = C$
- Apply option 1 on IDAL $\Rightarrow IDAL(i_1^{f_1}) = C, IDAL(i_2^{f_1}) = C, \cdots$

Functions contributing to highly critical FC (Cat) implemented by low development assurance level items (Major)

It's a lot of rules, is there another way to find an optimal allocation ?

DAL Allocation : Automatic allocation

DAL, FDAL & IDAL allocation problem is combinatorial problem :

- Real systems : hundreds of FCs & MCS with thousands of cuts !
  $\Rightarrow$ Nearly impossible to find optimal allocation by hand
- Presented rules are simplification of real allocation process (deal with failure modes, ...)
  $\Rightarrow$ Use constraint programming to allocate DAL [BDS11] for instance SAT or IDP).

DAL Allocation : Automatic allocation

Automatic problem generator needs :

- the MCS of FCs,
- the FC criticality,
- a partial or total independence relation,
- a cost function.

Result of the solver :

1. an optimal DAL allocation of function/items,
2. the completed independence relation used to compute the DAL allocation,
3. the downgrading options used.

DAL Allocation : Ask to IDP

Is the following allocation optimal ? ⇒ Ask to IDP

$$\{dist \mapsto C, srv \mapsto C, EMP \mapsto C, EDP \mapsto D, eng1 \mapsto C, elec \mapsto D\}$$

DAL Allocation : Ask to IDP

Is the following allocation optimal ? $\Rightarrow$ Ask to IDP $\Rightarrow$ No

$$\{dist \mapsto C, srv \mapsto C, EMP \mapsto C, EDP \mapsto D, eng1 \mapsto C, elec \mapsto D\}$$

basic DAL	cuts	DAL						Option
		$dist$	rsv	EMP	EDP	$eng1$	$elec$	
C	$\{dist\}$	$\geq$ C	-	-	-	-	-	-
	$\{rsv\}$	-	$\geq$ C	-	-	-	-	-
	$\{f_{EMP,eng1}, EDP\}$	-	-	$\geq$ C	$\geq$ E	-	-	1
	$\{f_{EMP,eng1}\}$	-	-	$\geq$ C	-	$\geq$ C	-	-
	$\{elec, EDP\}$	-	-	-	$\geq$ C	-	$\geq$ E	1
	$\{elec, f_{EMP,eng1}\}$	-	-	-	-	$\geq$ C	$\geq$ E	1
Result		$\geq$ C	$\geq$ C	$\geq$ C	$\geq$ C	$\geq$ C	$\geq$ E	
Cost		30						

Now a Recap

Today's lesson in 30"

Deal with dependencies

During design Trace independence assumptions during assessment ⇒ became requirements during implementation

During verification Identify the potential sources of dependencies & integrate them in safety assessment

Today's lesson in 30"

Emphasis on systematic errors :

- Currently, avoid systematic faults with design assurance level (DAL)
- DAL allocation depends on :
  - criticality of functions/items failures,
  - independence between them,
  - cost of DAL related activities.

You understand highlighted terms
$\Rightarrow$ congratulations you've got the idea
Otherwise check out the slides !

How to select the relevant safety framework ?

Dysfunctional model

Safety engineer creates **models** of the **failure propagation**

Formalises **contributions** of elementary failures to **feared events**

Derives **scenarios** leading to feared events thanks to a model based on a **formalism**

What a formalism can (or can't) **capture** ?

Static system

Definition (Static system)

The order of occurrence of the primary failures **does not** impact the occurrence of the studied feared event(s)

The scenarios leading to the feared event can modelled as **sets** :

- For instance by cutsets or prime implicants
- Can use many methods like Fault trees, Reliability block diagrams, HipHOPS, . . .
- Underlying formalism : propositional logic

Dynamic system

Definition (Dynamic system)

The order of occurrence of the primary failures impacts the occurrence of the studied feared event(s)

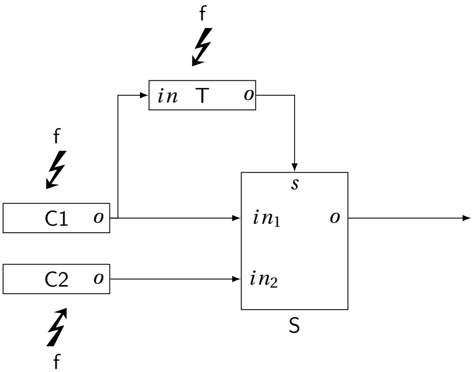
The scenarios leading to the feared event can modelled as **sequences** :

- For instance by minimal sequences or execution traces
- Can use many methods like Bayesian networks, Markov Chains, Petri Nets, ...
- Underlying formalism : State/Transition models

An example : the auto-check system

Assumptions :

- Data are correct or erroneous
- C1 (resp. C2) can produce erroneous outputs C1.o (resp. C2.o) if occurrence of C1.f (resp. C2.f)
- Test component sends true iff C1 output is correct
- Test can be permanently stuck on the last decision if T.f occurs
- Selector sends in1 if s is true, in2 otherwise
- Feared event is *Erroneous output on S.o*



Is the system dynamic or static ?

Deal with dynamism

Dynamic system models Either use a formalism dedicated to dynamic systems

- ⊕ Enable fine grain modelling of the failure propagation
- ⊕ Provide more meaningful analysis results
- ⊖ More complex to model and to analyse

Pessimistic model Build a pessimistic static model of your system

- ⊕ Easier to model and to analyse
- ⊖ Ensure that the model is pessimistic not always feasible

Build a dynamic model of the system : Markov chain

Definition (Markov chain)

Markov chain is a probabilistic state machine where :

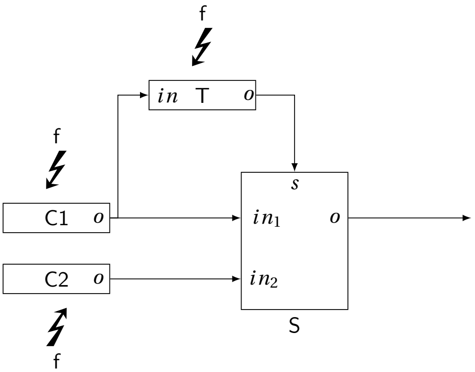
- States models the norminal or error system's states
- Transitions models the evolution of the system's state due to failures or nominal reconfigurations.
- A transition is labelled by a probability (for discrete MC, rate for continuous MC) of firing the transition from the current state.

Warning Applicable only if the system ensure the Markov assumption, i.e. the probability (or rate) of a transition depends only on the current state

An example : Markov chain for the auto-test system

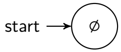
Instructions :

- A node of the chain encode the sequence (or set if the order does not matter) of component failed
- Transition are labeled by the failure rate of the event
- Initially none of the components are failed

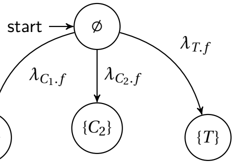


What is the Markov chain of this system ?

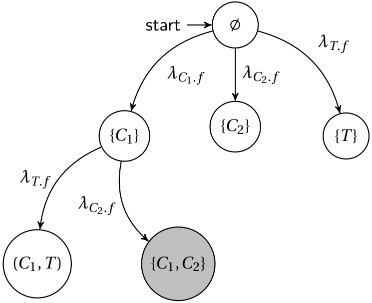
An example : Markov chain for the auto-test system



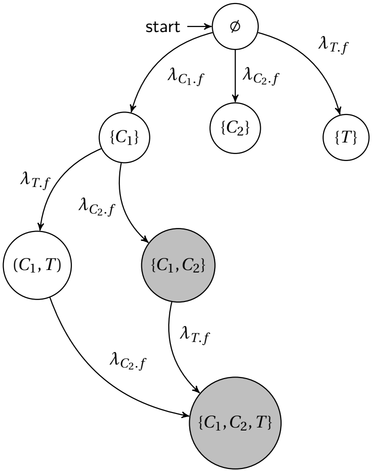
An example : Markov chain for the auto-test system



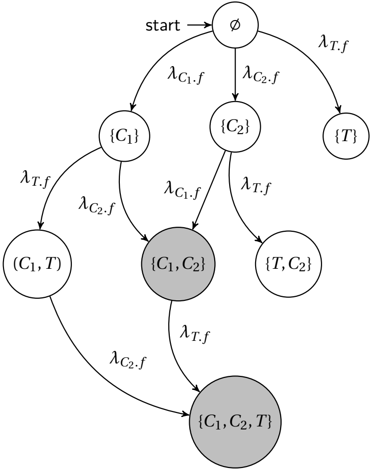
An example : Markov chain for the auto-test system



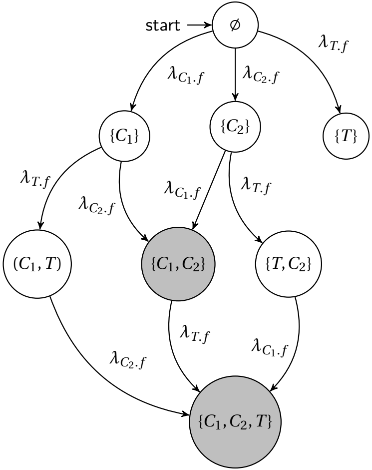
An example : Markov chain for the auto-test system



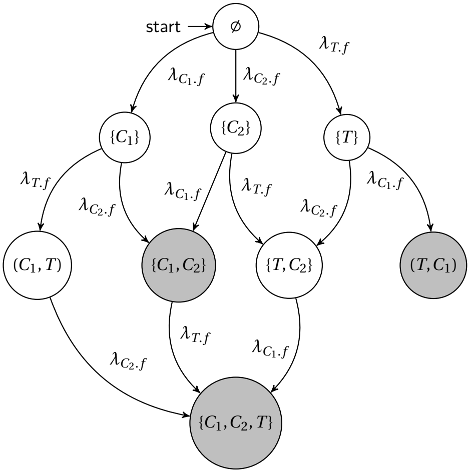
An example : Markov chain for the auto-test system



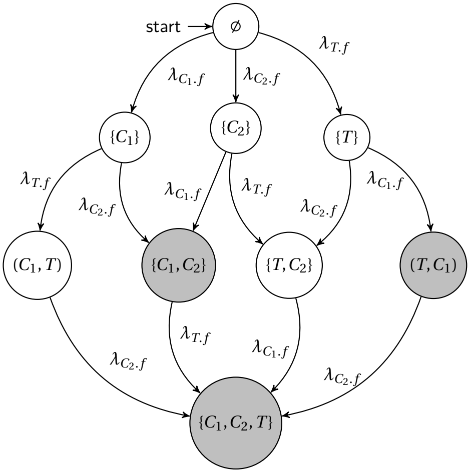
An example : Markov chain for the auto-test system



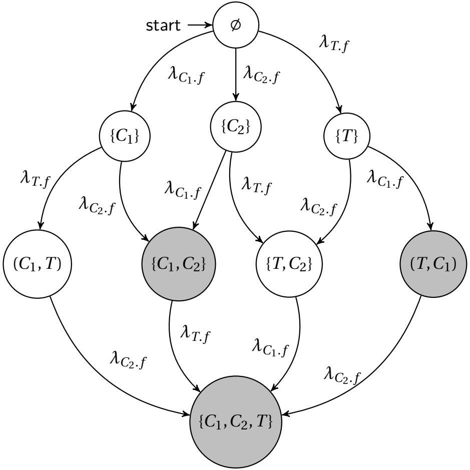
An example : Markov chain for the auto-test system



An example : Markov chain for the auto-test system



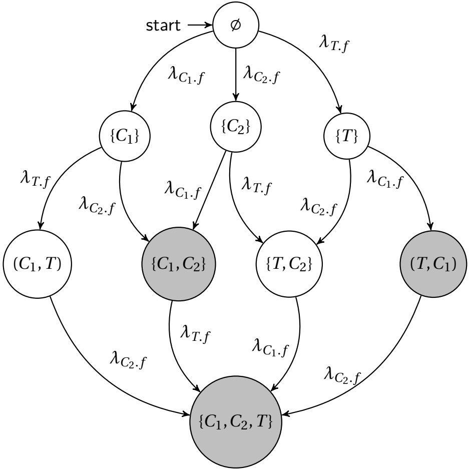
An example : Markov chain for the auto-test system



Possible analyses :

- Find sequences of events leading to a feared state
- Estimate the probability of a feared event with Monte Carlo method
- Ensure formal properties (with temporal logic)
- Ensure probabilistic properties (with probabilistic model checking)

An example : Markov chain for the auto-test system



Minimal Sequences

(C1.f,C2.f) ; (C2.f,C1.f) ; (T.f,C1.f)

Build a pessimistic model of the system

If one want to use a static model then it must ensure that the analysis is conservative

Definition (Conservative analysis)

If a sequence $(e_1, \dots e_n)$ leads to the failure, in the pessimistic model the set $\{e_1, \dots e_n\}$ leads to the failure.

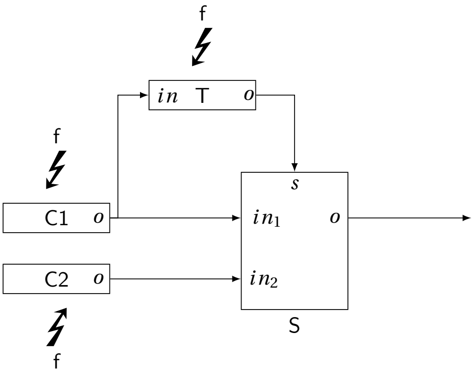
Example (Test component behavior)

In the auto-test system, assume that if the Test is failed then the selector will send an erroneous value if one of the element is failed.

An example : Fault tree for the auto-test component

Instructions :

- If the Test is failed then the selector will send an erroneous value if one of the element is failed.

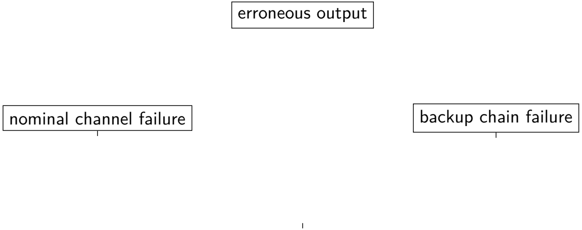


What is the fault tree of this system ?

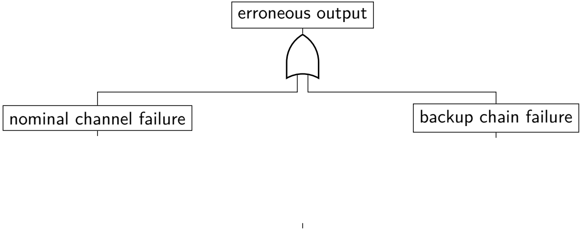
An example : Fault tree for the auto-test component

erroneous output

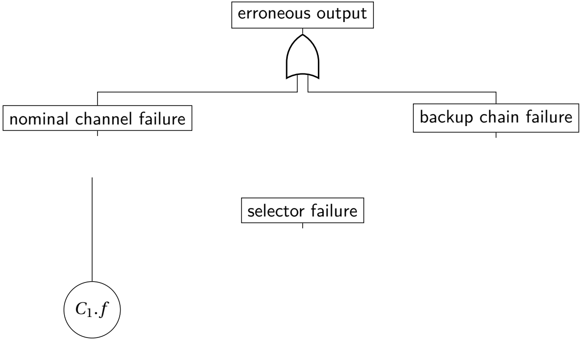
An example : Fault tree for the auto-test component



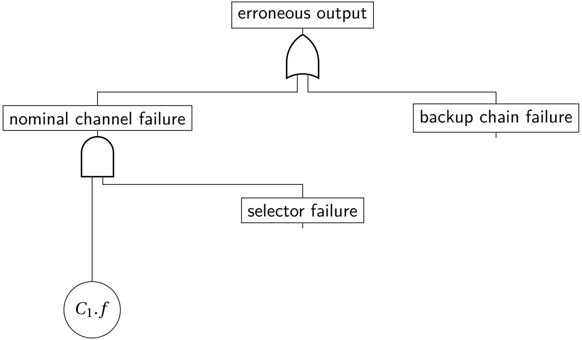
An example : Fault tree for the auto-test component



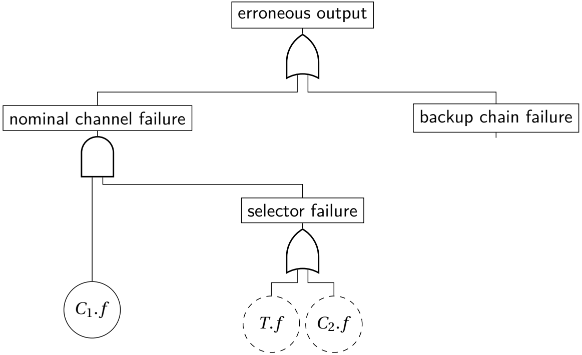
An example : Fault tree for the auto-test component



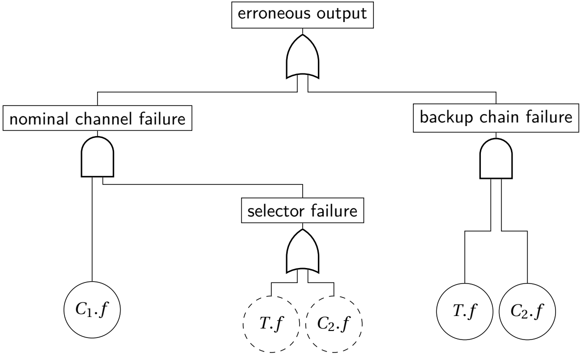
An example : Fault tree for the auto-test component



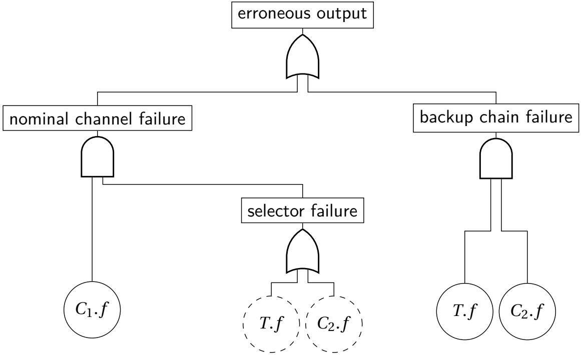
An example : Fault tree for the auto-test component



An example : Fault tree for the auto-test component



An example : Fault tree for the auto-test component



Minimal cutsets

$$\{\{C1.f, C2.f\};\{C1.f, T.f\};\{C2.f, T.f\}\}$$

Minimal sequences

$$(C1.f, C2.f);(C2.f, C1.f);(T.f, C1.f)$$

Limitations of classical formalism

Classic formalism shall highlight some failure propagation paths

- No explicit reference to the global system architecture / nominal behavior
- Potential misunderstanding or inconsistency between safety and design teams

Classical formalism totally relies on expert's analysis

- More and more difficult to be exhaustive for complex systems which integrate of various functions in a same hardware component
- Have reconfigurations of function modes and hardware architectures
- Are strongly interconnected with other systems

Perspectives

Goals provide

- Formal failure propagation models closer to design models
- Tools to assist construction and automated analysis of complex models

More details in the next lessons

Let's talk about the (your) future!

What are the new safety challenges ?

What are the new safety challenges ?

Let's have a quick (and non-exhaustive) overview !

From I to AI

Trend Huge trend to automate complex tasks preformed by operators (professional or not)

Breakdown New technologies involving complex sensor fusion or image processing

From I to AI

Trend Huge trend to automate complex tasks preformed by operators (professional or not)

Breakdown New technologies involving complex sensor fusion or image processing

What are the risks related to the massive adoption of such systems ?

An Example Automotive anti-collision system https://youtu.be/ZMFbMV5QNzk?t=81

Challenge 1 : Trust Me I Am Autonomous

- Classical software correctness demonstrated by :
  1. validation : the specification breakdown is sound, complete and testable (ABS example)
  2. verification : the implementation is compliant to the specification (Offshore example)
- V&V achieved thanks to testing, traceability and formal verification

Challenge 1 : Trust Me I Am Autonomous

- Classical software correctness demonstrated by :
  1. validation : the specification breakdown is sound, complete and testable (ABS example)
  2. verification : the implementation is compliant to the specification (Offshore example)
- V&V achieved thanks to testing, traceability and formal verification

What is the specification breakdown of an AI-based pedestrian detection system ?
How to provide confidence on safety integrity for critical function based on AI ?

Challenge 2 : Taking into account new failures

- Safety impact of hardware failure addressed in safety critical systems (redundancy, mutual checks, lock-step)

Challenge 2 : Taking into account new failures

- Safety impact of hardware failure addressed in safety critical systems (redundancy, mutual checks, lock-step)

What is the safety impact of an hardware failure executing AI-based software ?
Can we detect & manage this failure ?

Challenge 3 : Safe integration of tomorrow aircrafts

- Various applicative domains can benefit from new aircraft concepts (VTOL, UAV, ...)
  - Infrastructure inspection (SCNF, ERDF, ...)
  - Package delivery (Amazon, CDiscount, La Poste, ...)
  - Flying taxi (Airbus' Vahana project, Boeing, Uber, ...)

Challenge 3 : Safe integration of tomorrow aircrafts

- Various applicative domains can benefit from new aircraft concepts (VTOL, UAV, ...)
  - Infrastructure inspection (SCNF, ERDF, ...)
  - Package delivery (Amazon, CDiscount, La Poste, ...)
  - Flying taxi (Airbus' Vahana project, Boeing, Uber, ...)

What are the new risks related to the integration of such aircraft in the flight traffic ?
How to adapt safety analyses to take into account distributed procedures, autonomous avoidance systems ?

Thank you

ONERA

THE FRENCH AEROSPACE LAB

www.onera.fr