Optimal design of automated dependable system architectures

Application to a railroad transportation system

CLARHAUT Joffrey
Railroad vehicle transportation system

= Trucks on trains

• Advantages:
  – Decreasing congestion of roads
  – Less pollution and consumption
  – ...

• Need of dependability improvements:
  – Contributing to availability
  – Increasing of system’s safety
Concept of the smart wagon

Smart sensors integers functions like:

– monitoring,
– supervising,
– control,
– …
Concept of the smart wagon

Smart sensors integers functions like:
- monitoring,
- supervising,
- control,
- ...

Smart wagon
= instrumented wagon (sensors, actuators, ...) with the same functions of the smart sensor

Why a smart wagon?
- Link with other system’s parts
- Present in all system’s operational phases
Content

• Needs of a design methodology of automated systems
  – General concepts
  – Cuts and scenarii
  – Formalizations

• Presentation of the proposed design methodology
  – Modeling step
  – Optimization step
  – Case study

• Results
  – Comparison with traditional fault trees
  – Interest of scenarii

• Conclusion and future works
Designing a dependable system

Find a feasible architecture that guarantees an acceptable level of dependability

Available components

Needs

Criterion

Final architecture

Optimal design of automated dependable system

CLARHAUT Joffrey
System’s dependability level evaluation using scenarii

Cut:
sequence of failures that leads the system to a precise dreaded event

System S with two components

Active redundancy

Passive redundancy

Optimal design of automated dependable system

CLARHAUT Joffrey
System’s dependability level evaluation using scenarii

Cut:
sequence of failures that leads the system to a precise dreaded event

System S with two components

Active redundancy

System fails if
{ S1 fails, S2 fails }

Passive redundancy

System fails if
{ S1 fails, S2 fails }

Optimal design of automated dependable system

CLARHAUT Joffrey
System’s dependability level evaluation using scenarii

**Scenario:**

A time-ordered sequence of failures that leads the system to a precise dreaded event.

- **t=10:** Component failure
- **t=21:**
- **t=38:**
- **t=38:** Dreaded event
System’s dependability level evaluation using scenarii

Scenario:

A time ordered sequence of failures that leads the system to a precise dreaded event.

- **Component failure**
  - t=10
  - t=21
  - t=38

**Active redundancy**

- **S1**
- **S2**

- System fails if [ S1 fails, S2 fails ] or [ S2 fails, S1 fails ]

**Passive redundancy**

- **S1**
- **S2**

- System fails if [ S1 fails then S2 fails ]

Optimal design of automated dependable system

CLARHAUT Joffrey
Formalizations (1)

– A scenario ($\Psi_D$) is a time ordered sequence of $n$ failures that leads the system to a precise dreaded event ($D$)

$$\Psi_D = \left[ F_1, ..., F_n \right]$$

– A set of $m$ scenarios is denoted:

$$\Phi_D = \left\{ \Psi_D^1, ..., \Psi_D^i, ..., \Psi_D^m \right\}$$

– The length of a scenario from this set is denoted:

$$L(\Psi_D) = \text{card}(\Psi_D^i)$$

Optimal design of automated dependable system

CLARHAUT Joffrey
Formalizations (2)

- The minimal length of a set of scenarii ($\Phi_D$) is denoted:

$$L^D_{\text{min}} = \min_{1 \leq i \leq m} L(\Psi^i_D)$$

- The number of scenarii with minimal length is denoted:

$$N^D_{\text{min}} = \text{card}(\Delta_D) \text{ with } \Delta_D \subset \Phi_D$$

Dreaded event:

Caractérisé par:
- la longueur minimale ($L^D_{\text{min}}$)
- le nombre ($N^D_{\text{min}}$) de scenarii

Link with dependability:

Dependability level ($DL^S$) if

- $L^D_{\text{min}}$
- $N^D_{\text{min}}$
Design of a dependable automated system

Design methodology:
- Modeling step
- Optimization step
Design of a dependable automated system

Available components (sensors, actuators, …)

Component organizations

Design methodology:
- Modeling step
- Optimization step

- Dreaded events
- Failure modes

Set of optimal equipment architectures

Optimal design of automated dependable system

CLARHAUT Joffrey
Design of a dependable automated system

Design methodology:
- Modeling step
- Optimization step

Set of optimal equipment architectures

Available components (sensors, actuators, …)

Component organizations

Scenarii

Graphical models

- Dreaded events
- Failure modes

- Cost
- Dependability level

Optimal design of automated dependable system

CLARHAUT Joffrey
Design of a dependable automated system

- Methodology:
  1) Functional model
  2) Material architecture
  3) Combinatorial research + Evaluation

- Final result:
  Set of optimal architectures

Optimal design of automated dependable system

CLARHAUT Joffrey
Case study

Design of a fire protection system for the smart wagon

• **Two missions:**
  – Detect a fire
  – Send an alarm to operators (train driver, …).

• **Two dreaded events:**
  – No fire alarm when a fire is present (ER1).
  – False alarm (fire alarm without fire, ER2).

Evaluate a level of dependability and a financial cost
### Definition of basic components

<table>
<thead>
<tr>
<th>Basic component</th>
<th>Failure modes</th>
<th>Cost</th>
<th>Component possible organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>- Unexpected stop</td>
<td>5</td>
<td>- single component</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 2 components in active redundancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 2 components in passive redundancy</td>
</tr>
<tr>
<td>PLC</td>
<td>- Unexpected stop with alarm</td>
<td>3</td>
<td>- single component</td>
</tr>
<tr>
<td></td>
<td>- Unexpected stop without alarm</td>
<td></td>
<td>- 2 components with alarm priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 2 components without alarm priority</td>
</tr>
<tr>
<td>Heat detector</td>
<td>- Continuously active</td>
<td>1</td>
<td>- single component</td>
</tr>
<tr>
<td></td>
<td>- Continuously inactive</td>
<td></td>
<td>- 2 components in serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 2 components in parallel</td>
</tr>
<tr>
<td>Smoke detector</td>
<td>- Continuously active</td>
<td>1</td>
<td>- single component</td>
</tr>
<tr>
<td></td>
<td>- Continuously inactive</td>
<td></td>
<td>- 2 components in serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 2 components in parallel</td>
</tr>
</tbody>
</table>
Modeling step (1)

Functional model:

System’s hierarchical analysis represented by a tree with three types of nodes:

- Associative node:

- Alternative node:

- Elementary node:
Modeling step (2)

Fire protection system:

- Missions
  - No alarm
  - False alarm

- Use 1 control system
  - No alarm
  - False alarm

- Use 2 control systems
  - No alarm
  - False alarm

Detect fire:
Smoke AND heat
- No detection
- False detection

Detect fires
- No detection
- False detection

Detect fire:
Smoke THEN heat
- No detection
- False detection

Detect fire:
Smoke OR heat
- No detection
- False detection

Send an alarm
- No alarm
- False alarm

Send an alarm from PLC
- No alarm
- False alarm

Supply PLC
- No supply

Optimal design of automated dependable system
CLARHAUT Joffrey
Modeling step (2)

Fire protection system:

- Missions
  - No alarm
  - False alarm

- Use 1 control system
  - No alarm
  - False alarm

- Use 2 control systems
  - No alarm
  - False alarm

- Detect fire:
  - Smoke AND heat
    - No detection
    - False detection

- Detect fire:
  - Smoke THEN heat
    - No detection
    - False detection

- Detect fire:
  - Smoke OR heat
    - No detection
    - False detection

- Send an alarm
  - No alarm
  - False alarm

- Supply PLC
  - No supply

Optimal design of automated dependable system

CLARHAUT Joffrey
Modeling step (3)

Functional model of the fire protection system:

Detect fire: Smoke AND heat
Detect fire: Smoke THEN heat
Detect fire: Smoke OR heat

Detect heat
1 detector
2 serial detectors
2 parallel detectors

Heat detector

Detect smoke
1 smoke detector
2 serial detectors
2 parallel detectors

Smoke detector
Optimal design of automated dependable system

CLARHAUT Joffrey
Modeling step (4)

Improved multi-fault tree:

- Based on the previous functional model.
- Consists in associating to each node the set of failure modes that affect the accomplishment of the function.

Detect and notify fires
- No alarm (ER1)
- False alarm (ER2)

Detect fires
- No detection
- False detection

Send an alarm
- No alarm
- False alarm
Modeling step (4)

Improved multi-fault tree:

- Based on the previous functional model.
- Consists in associating to each node the set of failure modes that affect the accomplishment of the function.

Detect and notify fires
- No alarm (ER1)
- False alarm (ER2)

Detect fires
- No detection
- False detection

Send an alarm
- No alarm
- False alarm

\[ N_1 \left\{ \begin{array}{l}
\text{No detection OR No alarm } \Rightarrow \text{ER1} \\
\text{False alarm OR False detection } \Rightarrow \text{ER2}
\end{array} \right. \]
Missions of operators:

- Represent relations between different failures in the modeling step.
- Apply computational properties in the optimization step.
Missions of operators:
- Represent relations between different failures in the modeling step.
- Apply computational properties in the optimization step.

Classical operators:
- AND
- OR

Temporal operators:
- AND-Priority (PAND)
- Sequential (SEQ)

System fails if S1 fails then S2 fails
Examples of computational properties:

- Let A, B and C, three dreaded events and $\Delta_A$, $\Delta_B$ and $\Delta_C$ the three sets of minimal scenarios.
- C results from the association of A and B with one of the previous operators.

\[
L^C_{\text{min}} = L^A_{\text{min}} + L^B_{\text{min}}
\]

For C = A AND B:

\[
N^C_{\text{min}} = \frac{(L^A_{\text{min}} + L^B_{\text{min}})!}{L^A_{\text{min}}! \times L^B_{\text{min}}!} \times N^A_{\text{min}} \times N^B_{\text{min}}
\]

\[
L^C_{\text{min}} = L^A_{\text{min}} + L^B_{\text{min}}
\]

For C = A PAND B:

\[
N^C_{\text{min}} = \frac{((L^A_{\text{min}} - 1) + L^B_{\text{min}})!}{(L^A_{\text{min}} - 1)! \times L^B_{\text{min}}!} \times N^A_{\text{min}} \times N^B_{\text{min}}
\]

\[
L^C_{\text{min}} = L^A_{\text{min}} + L^B_{\text{min}}
\]

For C = A SEQ B:

\[
N^C_{\text{min}} = N^A_{\text{min}} + N^B_{\text{min}}
\]
Modeling step (6)

Fire protection system:

- Missions
  - No alarm
  - False alarm

- Use 1 control system
  - No alarm
  - False alarm

- Use 2 control systems
  - No alarm
  - False alarm

- Detect fires
  - No detection
  - False detection

- Detect fire:
  - Smoke AND heat
    - No detection
    - False detection

- Detect fire:
  - Smoke THEN heat
    - No detection
    - False detection

- Detect fire:
  - Smoke OR heat
    - No detection
    - False detection

- Send an alarm from PLC
  - No alarm
  - False alarm

- Supply PLC
  - No supply

Optimal design of automated dependable system

CLARHAUT Joffrey
Modeling step (6)

Fire protection system:

- Missions:
  - No alarm
  - False alarm

- Use 1 control system:
  - No alarm
  - False alarm

- Use 2 control systems:
  - No alarm
  - False alarm

- Detect fire:
  - Smoke AND heat
    - No detection
    - False detection

- Detect fire:
  - Smoke THEN heat
    - No detection
    - False detection

- Detect fire:
  - Smoke OR heat
    - No detection
    - False detection

- Detect fires:
  - No detection
  - False detection

- Send an alarm:
  - No alarm
  - False alarm

- Supply PLC:
  - No supply

Dreaded events

Optimal design of automated dependable system

CLARHAUT Joffrey
Modeling step (7)

Fire protection system:

- Missions
  - No alarm
  - False alarm

- Use 1 control system
  - No alarm
  - False alarm

- Use 2 control systems
  - No alarm
  - False alarm

- Detect fires
  - No detection
  - False detection

- Detect fire:
  - Smoke AND heat
  - No detection
  - False detection

- Detect fire:
  - Smoke THEN heat
  - No detection
  - False detection

- Detect fire:
  - Smoke OR heat
  - No detection
  - False detection

- Send an alarm from PLC
  - No alarm
  - False alarm

- Supply PLC
  - No supply

Optimal design of automated dependable system

CLARHAUT Joffrey
Fire protection system:

Missions
- No alarm
- False alarm

Use 1 control system
- No alarm
- False alarm

Use 2 control systems
- No alarm
- False alarm

Detect fires
- No detection
- False detection

Detect fire:
- Smoke AND heat
- No detection
- False detection

Detect fire:
- Smoke THEN heat
- No detection
- False detection

Detect fire:
- Smoke OR heat
- No detection
- False detection

Send an alarm from PLC
- No alarm
- False alarm

Supply PLC
- No supply

N3

Failure relationships

No detection OR No alarm ⇒ ER1
False alarm OR False detection ⇒ ER2

Optimal design of automated dependable system
CLARHAUT Joffrey
Optimisation step

Fire protection system:

- Missions
  - No alarm
  - False alarm

- Use 1 control system
  - No alarm
  - False detection

- Use 2 control systems
  - No alarm
  - False detection

- Detect fires
  - No detection
  - False detection

- Detect fire:
  - Smoke AND heat
  - No detection
  - False detection

- Detect fire:
  - Smoke THEN heat
  - No detection
  - False detection

- Detect fire:
  - Smoke OR heat
  - No detection
  - False detection

- Send an alarm
  - No alarm
  - False alarm

- Supply PLC
  - No supply

Optimal design of automated dependable system

CLARHAUT Joffrey
Optimal design of automated dependable system

CLARHAUT Joffrey
Optimisation step

Fire protection system:

- **Use 1 control system**
  - No alarm
  - False alarm

- **Use 2 control systems**
  - No alarm
  - False alarm

- **Detect fires**
  - No detection
  - False detection

- **Detect fire:**
  - Smoke AND heat
  - No detection
  - False detection

- **Detect fire:**
  - Smoke THEN heat
  - No detection
  - False detection

- **Detect fire:**
  - Smoke OR heat
  - No detection
  - False detection

- **Send an alarm from PLC**
  - No alarm
  - False alarm

- **Supply PLC**
  - No supply

Optimal design of automated dependable system

CLARHAUT Joffrey
Optimisation step

Fire protection system:

**Missions**
- No alarm
- False alarm

**Use 1 control system**
- No alarm
- False alarm

**Use 2 control systems**
- No alarm
- False alarm

**Detect fires**
- No detection
- False detection

**Detect fire:**
- Smoke AND heat
  - No detection
  - False detection

**Detect fire:**
- Smoke THEN heat
  - No detection
  - False detection

**Detect fire:**
- Smoke OR heat
  - No detection
  - False detection

**Send an alarm**
- No alarm
- False alarm

**Supply PLC**
- No supply

Non optimal system

New system to insert

Optimal design of automated dependable system

CLARHAUT Joffrey
Fire protection system:

\[ \Omega_{\text{optimal}} = 31 \text{ optimal control architectures} \]

<table>
<thead>
<tr>
<th>Number of optimal systems and costs</th>
<th>( L_{\text{min}} ) for dreaded event: false alarm (ER2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>( L_{\text{min}} ) for dreaded event: No fire alarm (ER1)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2 systems C: 10</td>
</tr>
<tr>
<td></td>
<td>2 systems C: 13 to 19</td>
</tr>
<tr>
<td></td>
<td>2 systems C: 20</td>
</tr>
</tbody>
</table>
Comparison with traditional fault trees

• Traditional fault trees:
  – The three types of nodes are used.
  – Only OR and AND operators are used.

• Methodology results:
  \( \Omega'_{\text{optimal}} = 54 \) optimal control architectures.

Solutions obtained with the improved multi-fault tree are better: evaluation without the impossible scenarii
Interest of scenarii

Example of optimal architecture:

Optimal design of automated dependable system
CLARHAUT Joffrey
Interest of scenarii

Example of optimal architecture:

Number of minimal scenarii ($N_{\text{min}}$) for dreaded event « No fire alarm » (ER1):
- Traditional evaluation method: 18
- Proposed evaluation method: 12

Impossible scenario: [Unex. Stop of power supply 2, Unex. Stop of power supply 1, Unex. Stop of power supply 3]

Optimal design of automated dependable system

CLARHAUT Joffrey
Conclusion

- **Methodology interests:**
  - System’s models using scenarii.
  - Set of optimized architectures characterized by a financial cost and a dependability level.
  - Can be used in the first design phases
    - obtain a first estimation of cost,
    - determine a first set of architectures.

- **Future works:**
  - Using several types of basic components (standard, smart and safe) with relative reliability coefficient.
  - Improve algorithms for huge systems.
  - Design of a software.
Optimal design of automated dependable system architectures

Application to a railroad transportation system

Thank you!!

CLARHAUT Joffrey
joffrey.clarhaut@inrets.fr