Customer satisfaction (Reliability)
VS
Safety

Aspects of Reliability and Safety

Tord Wullt 2016

addalot
QUALITY IMPROVEMENT

Reliability and safety

- Often reliability is in conflict with safety
  - Safe state with degraded functionality is used

- Safety and reliability can be in synergy
  - If only full functionality is safe, then there is no conflict

- How can safety be combined with good reliability?

Reliability and safety

Workshop purpose

- Discuss how to improve or secure reliability of safety related solutions

Tord Wullt addalot partner

- Master of Science, applied physics LTH
  - **TUV Rheinland certified FSE Automotive ISO26262**
  - Scrum Master
- System and SW development

- **Functional safety related**
  - **Automotive 5 yrs, Volvo Cars and Volvo trucks**
    - Dependability/Reliability, Active safety, Power train, Certification to EU regulations
    -
  - **Offshore energy and Maritime 7yrs: Det Norske Veritas**
    - Offshore Energy, Complex System quality and safety

  - **Defense industry Telub, BT/Toyota, SAAB Military Aircrafts**
    - Automation, Functional Safety

addalot
QUALITY IMPROVEMENT

Reliability and safety

How ISO26262 and related standards care about reliability:

- Cares about reliability to not violate Safety Goals
- Does not care if safe states are entered to often
- Does not drive reliability of other goals than of Safety Goals
- When Safety Goals are the same as Reliability goals then OK!

Reliability and safety

Discussion Background:

- Organizations are sometimes immature in applying a standard like ISO26262
- Organizations have long experience in their field of solutions and have a reliable established design and development process
- With ISO26262 there are new requirements and it is easy to loose control of reliability
  - New unfamiliar design elements
  - New activities
  - Competence on few hands
    - Topic experts does not dare to question Safety decisions
    - Safety work not integrated in the development process and a holistic view of reliability may be hindered
  - Limited competence and budget.
    - Safety solution is pushed to be as simple as possible giving safety, but some times with unnecessary impact on reliability

Reliability and safety

Supplier management

ISO26262 requirements combined with weak reliability requirements

- tend to result in safety solutions that have unnecessary high impact on reliability, especially if the competence and experience is weak.

The supplier need requirements to work with reliability in a systematic manner as with 26262

- OEM need to identify reliability goals and acceptable degradation that minimize the negative customer effect, and provide this to the supplier
- The supplier is required to work systematically to prevent violation of reliability goals – FMEA, FTA on different levels in analogy to 26262
- Reliability Analysis shall include safety mechanisms!

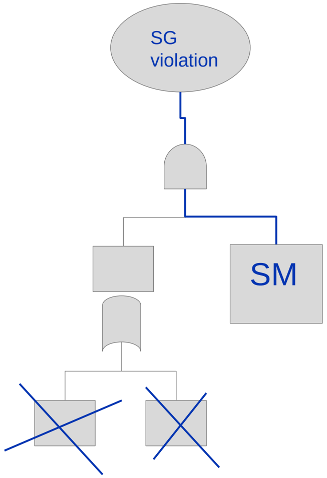
Reliability and safety

Some examples how to improve reliability of the normal function when a safe state with degraded functionality is used

Reliability and safety

Improve the reliability of the normal function

- Eliminate the causes for the safety related malfunction
  - Understand the causes for the failure that the Safety Mechanism detects, use FTA and FMEA
  - Eliminate the causes by
    - redundancy
    - improved components
    - improved quality assurance
    - etc.
- If a failure still occur, the safety mechanism will assure safety

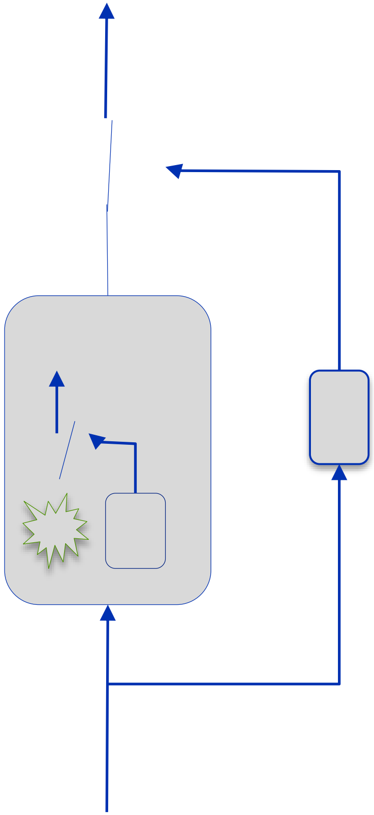


- Pro:
  - More reliable normal function
  - No effect on safety solution
  - Safe state with reliability impact can be used
- Con:
  - More costs for development and HW

Reliability and safety

Preventive normal function

- The normal function detects and mitigates safety related failures before the Safety Mechanism take action
  - Detect lower events and makes e.g. reset
  - Degrades the function to avoid the hazard
- Within Fault Tolerant Time Interval
- If a failure still occur, the safety mechanism will assure safety

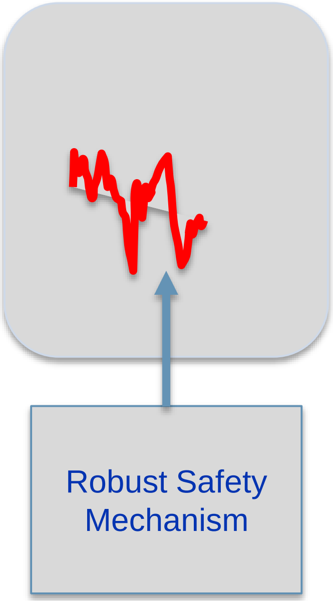


- Pro:
  - More reliable normal function
  - No effect on safety solution
  - Safe state with reliability impact can be used
- Con:
  - More costs for development and HW

Reliability and safety

Robust Safety Mechanism

- False detections have direct impact on reliability
- High diagnostic coverage and few false detections may be in conflict
- Use FTA to analyze causes to the Safety Mechanism failure
  - Can root causes be taken away?
- Utilize the full FTTI to make a good filtering
- Estimate the Fault frequency of the Safe mechanism and check that it is acceptable
  - Simulations and statistical analysis
- Maybe a change of safety strategy is needed so that the Safety Mechanism robustly can detect another failure



Robust Safety Mechanism

- Pro: More reliable normal function
- Con: More complex safety mechanism, risk for lower diagnostic coverage

Reliability and safety

More specific Hazard analysis

- To have more specific situations and failure modes can lead to Safety Goals allowing for less impact on reliability.
- E.g.: Driving.
  - To differentiate driving at high speed and low speed.
  - Driving in low speed may not be safety related.

Exposure

Severity

Controllability

- Pro: More reliable normal function
- Con: Possibly more complex safety solution

Reliability and safety

More specific Safe states

- Often a safe state is chosen because it is a easy to implement like ”shut down”
- Safe states can some times be more specific allowing for a degraded service instead of ”shut down”

- Pro: More reliable normal function
- Con: More complex safety solution

Reliability and safety

Several Safe states – degradation strategy

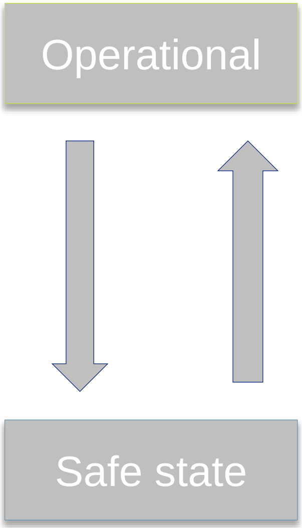
- Instead of one “all covering” safe state, you can have several safe states to minimize the reliability impact in a given situation

- Pro: More reliable normal function
- Con: More complex safety solution

Reliability and safety

Recover from safe state

- Allow to recover from safe state, if possible
  - If the failure mode heals, spontaneously or after reset etc.

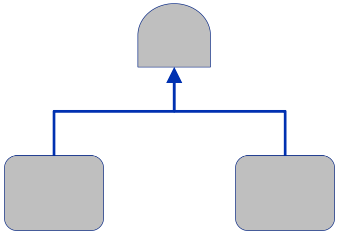


- Pro: More reliable normal function
- Con: More complex safety solution

Reliability and safety

Multiple point failure

- Utilize latent fault detection interval (possibly one drive cycle)
  - Sometimes latent fault detection interval is not utilized because it is easier to use one ”shut down” strategy
  - ASIL decomposition will create multiple point failures and improve reliability



- Pro: More reliable normal function
- Con: More complex safety solution

Reliability and safety

- More ways?
- Discussion