A Vision-based Dynamic Failsafe Architecture

Functional Safety Concept Considerations and Research Goals

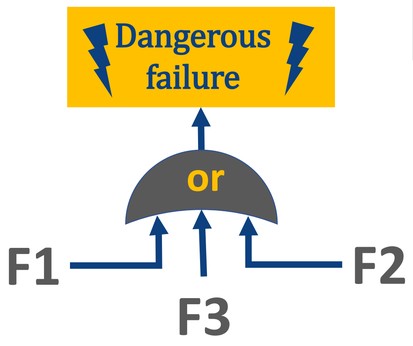
Authors: Amer Kajmakovic[1], Valon Osmani[2], Konrad Diwold[1], Nermin Kajtazovic[2], Robert Zupanc[2], Simon Mayer[1,3]
[1] Pro2Future GmbH and Graz University of Technology, Graz, Austria , [2] Siemens AG Österreich, Graz, Austria, [3] University of St. Gallen, St. Gallen, Switzerland
email: amer.kajmakovic@pro2future.at ; valon.osmani@siemens.at

Note: This approach shows some relevant aspects of the overall safety concept only. The demonstrator has been realized to evaluate different safety measures, but no assumptions can be made on its quality or functional safety (e.g. SC/SIL level acc. to IEC61508:2010). The ongoing research work is focused towards establishing a solid safety concept for dynamically reconfigurable failsafe architecture. Safety analysis of imaging/vision systems and possible failure modes that may arise from those systems are of particular interest here.

Analysis: Types of Hazards and Risks

F1 Simatic system

Dangerous failures in the Simatic system (e.g. RAM fault). Due to failsafe architecture and high diagnostic coverage of self-tests, the failure rate is guaranteed at SIL3 (PFD < 10E-05, PFH < 1E-10, …)



F2 Data Transmission

Errors occur due to transmission, timing and data integrity:

- Data does not arrive (Transmission failure)
- Data arrives late (Transmission delay)
- Data does not arrive in correct sequence (Out of order delivery) …

F3 Detection and classification

Errors might occur due to malfunctions in the camera or the image classification system.

Situation	Classification	Consequences
Presence	Presence detected	
Object is there	Yes	No Failure
Object is not there	No	No Failure
Object is there	**No**	**Safety function dangerously affected**
Object is not there	**Yes**	**Safety function dangerously affected**

Type of Failures in detection and classification:

- **Random hardware failures[1]**
  Failures due to problems with image sensor (photo-sensitive pixels)
- **Systematic failures[2]**
  Failures due to problems as noise in the images, bias, shadows, glare, reflections, low contrast, occlusions…

Safety Requirements

R1 Requirements are already implemented for F-I/O and F-CPU by **Siemens – SIL3 applications**

R2 The system must detect the typical **communication related failures**: corruption, repetition, incorrect sequencing, loss of messages, insertion, masquerade, addressing, out-of-sequence..

R3

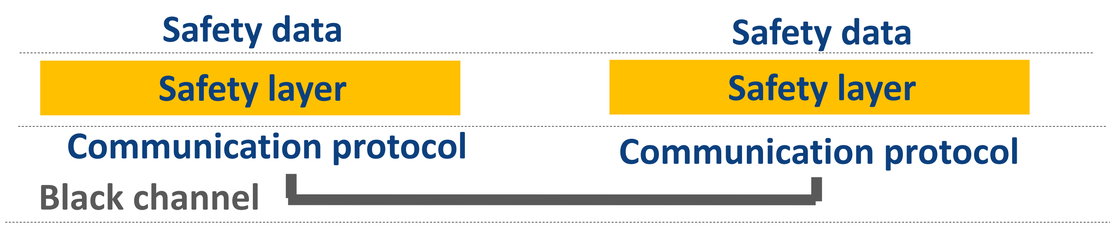
- System must maintain the safe state if any failure occurs during the object detection.
- System needs to be capable to deal with two main categories of the failures: **random hardware failures** and **systematic failures** mentioned before.

Future Investigations:
(a) how random hardware failures may affect the classification,
(b) how systematic failures may lead to the wrong classification (image processing).

Safety Measures

M1 No need for special safety measure, F-devices already have all required measures!

M2 A **black channel architecture** has been proposed to detect the communication related failures (e.g. timing of image delivery is monitored by watchdog mechanisms).



Threat	Defenses			
	Sequence number	Time stamp	Time-out	Cryptographic techniques
Repetition	X	X		
Deletion	X			
Insertion	X			
Re-sequence	X	X		
Corruption				X
Delay		X	X	
Masquerade				X

Standards connected to safety networking: IEC61508:2010-2; IEC 61784-3-3; IEC 62280

M3 Relevant research topics/goals to overcome random hardware failures and systematic failures:

- Safety analysis of hardware architectures for **image sensors** (with higher SIL/ASIL/... including component failure data, e.g. Sony IMX324 with ISO22626:2011 ASIL B).
- Analysis of possible failure modes that may come from object recognition within the imaging system (e.g. **Computer Vision Hazard and Operability Analysis - CV-HAZOP**).
- Explicit **image quality detection rules** need to be applied. These rules shall serve to characterize valid operational profile of image sensors.

References:

1. On Semiconductor: Evaluating Functional Safety in Automotive Image Sensors, TND6233/D Rev. 1, MAY - 2018
2. Oliver Zendel, Markus Murschitz, Martin Humenberger, Wolfgang Herzner: How Good Is My Test Data? Introducing Safety Analysis for Computer Vision. International Journal of Computer Vision 125(1-3): 95-109 (2017)
3. O. Zendel, M. Murschitz, M. Humenberger and W. Herzner, "CV-HAZOP: Introducing Test Data Validation for Computer Vision," 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, 2015, pp. 2066-2074.
4. Johann Thor Mogensen Ingibergsson, Dirk Kraft, and Ulrik Pagh *Explicit Image Quality Detection Rules for Functional Safety in Computer Vision* Institute University of Southern Denmark 28 November 2016