The Project: Wireless Fire Alarm System

• Develop new communication protocol for wireless fire alarm systems (WFAS).

  • Main functionality:
    • Self-monitoring (display non-operational sensors at central unit)
    • Alarm notification (display fire indications (smoke, heat, etc.) at central unit)

  • Timing constraints are regulated by European Norm EN 54, Part 25.

  • Goal: satisfy EN 54-25 — and have a good, robust, efficient overall product.

Situation

• Wireless Fire Alarm Systems exist and are available on the market.
• Most parts (like smoke / heat sensors) are already regulated by EN 54.
• Part 25 of EN 54 (for wireless FAS) just released:
  • Requirements are given as natural language text.
  • Requirements are the basis of certification tests (certification authorities test products and may issue EN 54 conformance confirmations).
• The new WFAS will be the first one to be subject to certification test.
  → clarification of requirements (with certification authority) necessary.
• Design ideas for the communication protocol exist.
  → design ideas need to be checked against (clarified) requirements.
• Being an SME does not imply not developing (safety-)critical systems.

• SME are often vulnerable to risks such as:
  • failed projects, (extra cost)
  • delayed projects, (extra cost, time-to-market)
  • defective products, (product liability)

Large-sized enterprises often much less, cf. VW, Intel, ... 

• SME are thus often hesitant to implement changes, in particular in the development process.
Die Anwendung eines der in 8.2.7 definierten HF-Störsignale auf einen der BMA-Empfänger darf weder einen Alarmzustand noch einen Störungsmeldezustand an der BMZ erzeugen.

4.2.5.2 Verfügbarkeit der HF-Verbindung in zwei oder mehr technisch ähnlichen Anlagen des
Let $T$ be the test mon.

If $\exists j \in J$ such that $T \not\subset T_j$ or if $\exists j \in J$ such that $\text{FailPers}_i \not\subset \text{NoFail}_i$, then $T \not\subset T_j$.

1: \{ 

1. JAM •

• an alarm condition.

for observables $n, \leq \leq (\text{for frequency bands})$

1. \{ $T_i \not\subset \text{FAIL}_i$ when $\text{Pers}_i \not\subset \text{NoPers}_i$.

\text{displayed} No spurious

$\text{ready for use}$ —

We assume the following

$n, \leq \leq (\text{for frequency bands})$

1. \{ $T_i \not\subset \text{FAIL}_i$ when $\text{Pers}_i \not\subset \text{NoPers}_i$.

\text{displayed} No spurious

$\text{ready for use}$ —

We assume the following

$n, \leq \leq (\text{for frequency bands})$
compare expected outcome and real outcome.

**detection means:** master knows effective 400 s between 'sensor gone' and 'message at central unit'

\[ s \in I \]

\[ \ell = \text{DISP} \land \neg \text{DET} \left[ \left( \bigwedge, \text{tell} \right) \right] \]

\[ i \leq \text{DET} \]

fail: invalid

• invalid

• effective 300 s between 'sensor gone' and 'message at central unit'

\[ s = \text{FAIL} \land (R1) \]

\[ \text{evolution} \]

\[ \text{of (R1)} \]

\[ \text{with repeaters:} \]

• plausible interpretations

\[ 3 \]

misses the sensor

master does not

satisfy the requirements, we have

formal representation: teach DC (usually not economic).

bullet points:

- Design Modelling
- Model Architecture, Validation
- Analysis, Formalisation, Validation
- Requirements Engineering
- Formal Methods in the Development Process
- Model Decomposition, Resource Consumption

bullet points:

- System Requirements: Alarm

bullet points:

- TestArchitecture

bullet points:

- Validation

bullet points:

- System Requirements: Alarm

bullet points:

- TestArchitecture

bullet points:

- Validation
Example: Detect / Display (Cont'd)

- Detection means: central unit knows effectively 300 s between 'sensor gone' and 'message at central unit'.
- Detection not really important effectively 400 s between 'sensor gone' and 'message at central unit'.
- Detection means: master knows then check every 300 s. and have 100 s to transport information to central unit.

Content

Wireless Fire Alarm System

Situation at Project Start

New Regulation of Wireless Fire Alarm Systems

Small-to-medium-sized Enterprises

Formal Methods in the Development Process

Requirements Engineering

Analysis, Formalisation, Validation

Design Modelling

Model Architecture, Validation

Verification

Model Decomposition, Resource Consumption

Conclusion

For a complete mechanized description of the project's situation, we start with an overview of the project's context.

For formal behavioural models, we employ a TDMA scheme for time division multiple access.

Periodically, each sensor sends a "hi master, I'm still here" message to its master. If a master misses that message from one of its sensors: report incidence.

To avoid message collision, we employ a TDMA scheme.

Sensor 1 says "I'm here" to its master.
Alarm Forwarding:
Whenever a sensor detects an indication of fire (smoke, heat, etc.), it sends out an ALARM message. This message is immediately acknowledged and forwarded by the sensor's master to its master, and so on, until the ALARM message reaches the central unit.

What if two sensors detect indications of fire at the same point in time? "Message collision" (both send at the same time).
Collision resolution ('tree splitting' protocol):

The Project:
Wireless Fire Alarm System
Situation at Project Start
New Regulation of Wireless Fire Alarm Systems
Small-to-medium-sized Enterprises
Formal Methods in the Development Process
Requirements Engineering
Analysis, Formalisation, Validation
Design Modelling
Model Architecture, Validation
Verification
Model Decomposition, Resource Consumption

Conclusion
From DC Formula to Queries: Self-Monitoring

• Queries:
  - E<> switcher.DETECTION sanity-check: "it is possible to detect one missing sensor" (check with sensor switcher and with channel blocker)
  - A[] not deadlock sanity-check: no deadlock
  - A[] (switcher.DETECTION imply switcher.timer <= 300*Second) requirement: "detection takes at most 300 s" (check with sensor switcher and with channel blocker)
  - A[] !center.ERROR requirement: "no spurious errors" (check without sensor switcher, with channel blocker)

References
