Real-Time Systems

Lecture 20: Formal Methods for Timed Systems in SME

2018-02-01

Dr. Bernd Westphal

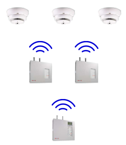
Albert-Ludwigs-Universität Freiburg, Germany

Content

- **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**

The WFAS Project

The Project: Wireless Fire Alarm System



(Arenis et al., 2016)

- Develop new **communication protocol** for **wireless fire alarm systems** (WFAS).
- **Main functionality**:
  - **self-monitoring**, and
    (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

Project Context (at project start)

- 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.

Small-to-Medium-sized Enterprises (SME)

- **SME**: small-to-medium sized enterprise

	small sizes	medium sized	other medium-sized
employees	≤ 50	≤ 250	≤ 500
turnover per year or	≤ 10 Mio. €	< 50 Mio. €	≤ 50 Mio. €
total per year ("Jahresbilanzsumme")	up to 10 Mio. €	≤ 43 Mio. €	≤ 43 Mio. €

`https://www.zim-bmwi.de/unternehmenstyp.pdf`

- 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, …)

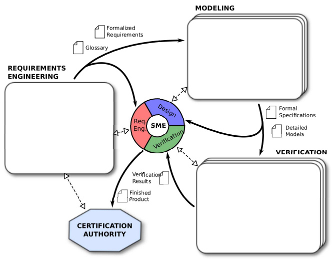
- SME are thus often **hesitant** to implement **changes**, in particular in the **development process**.

Content

- **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**

Process

Formal Methods for SME

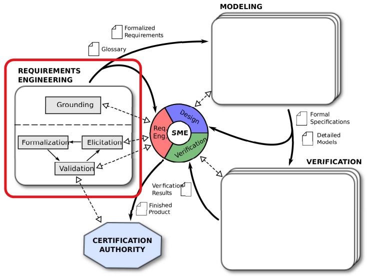


Content

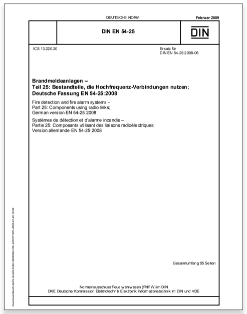
- **The Project**
  - **Wireless Fire Alarm System**
- **Situation at Project Start**
  - **New Regulation** of Wireless Fire Alarm Systems
  - **Small-to-medium-sized Enterprises**
- **Formal Methods in the Development Process**
  - **Requirements Engineering**
    - Analysis, Formalisation, Validation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

Requirements

Formal Requirements Engineering



The Starting Point: EN 54-25



DEUTSCHE NORM **Februar 2009**

DIN EN 54-25 DIN

ICS 13.220.20

Ersatz für
DIN EN 54-25:2008-06

Brandmeldeanlagen –
Teil 25: Bestandteile, die Hochfrequenz-Verbindungen nutzen;
Deutsche Fassung EN 54-25:2008

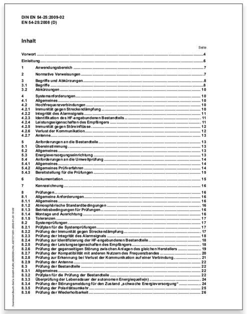
Fire detection and fire alarm systems –
Part 25: Components using radio links;
German version EN 54-25:2008

Systèmes de détection et d'alarme incendie –
Partie 25: Composants utilisant des liaisons radioélectriques;
Version allemande EN 54-25:2008

Gesamtumfang 55 Seiten

Normenausschuss Feuerwehrwesen (FNFW) im DIN
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

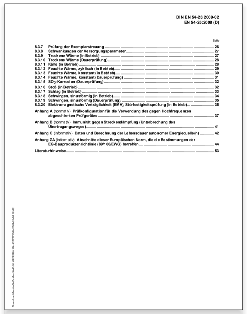
The Starting Point: EN 54-25



DIN EN 54-25:2009-02
EN 54-25:2008 (D)

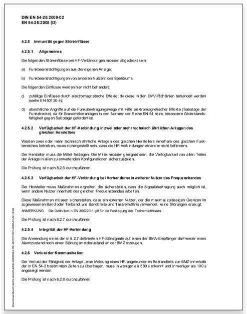
Inhalt

The Starting Point: EN 54-25



DIN EN 54-25:2009-02
EN 54-25:2008 (D)

The Starting Point: EN 54-25



DIN EN 54-25:2009-02
EN 54-25:2008 (D)

4.2.5 Immunität gegen Störeinflüsse

4.2.5.1 Allgemeines

Die folgenden Störeinflüsse bei HF-Verbindungen müssen abgedeckt sein:

a) Funkbeeinträchtigungen aus der eigenen Anlage;

b) Funkbeeinträchtigungen von anderen Nutzern des Spektrums.

Die folgenden Einflüsse werden hier nicht behandelt:

c) zufällige Einflüsse durch elektromagnetische Effekte, da diese in den EMV-Richtlinien behandelt werden (siehe EN 50130-4);

d) absichtliche Angriffe auf die Funkübertragungswege mit Hilfe elektromagnetischer Effekte (Sabotage der Funkstrecke), da für Brandmeldeanlagen in den Normen der Reihe EN 54 keine besondere Widerstandsfähigkeit gegen Sabotage gefordert ist.

4.2.5.2 Verfügbarkeit der HF-Verbindung in zwei oder mehr technisch ähnlichen Anlagen des gleichen Herstellers

Werden zwei oder mehr technisch ähnliche Anlagen des gleichen Herstellers innerhalb des gleichen Funkbereiches betrieben, muss sichergestellt sein, dass die HF-Verbindungen einander nicht behindern.

Der Hersteller muss die Mittel festlegen. Die Mittel müssen geeignet sein, die Verfügbarkeit von allen Teilen der Anlage in allen zu erwartenden Konfigurationen sicherzustellen.

Die Prüfung ist nach 8.2.6 durchzuführen.

4.2.5.3 Verfügbarkeit der HF-Verbindung bei Vorhandensein weiterer Nutzer des Frequenzbandes

Der Hersteller muss Maßnahmen ergreifen, die sicherstellen, dass die Signalübertragung auch möglich ist, wenn andere Nutzer innerhalb des gleichen Frequenzbandes arbeiten.

Diese Maßnahmen müssen sicherstellen, dass ein externer Nutzer, der die maximal zulässigen Grenzen im zugewiesenen Band oder Teilband, wie Bandbreite und Tastverhältnis verwendet, keine Störungen erzeugt.

ANMERKUNG Die Definiton in EN 300220-1 gilt für die Festlegung des Tastverhältnisses.

Die Prüfung ist nach 8.2.7 durchzuführen.

4.2.5.4 Integrität der HF-Verbindung

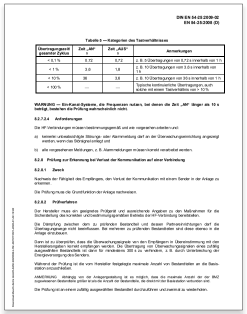
Die Anwendung eines der in 8.2.7 definierten HF-Störsignale auf einen der BMA-Empfänger darf weder einen Alarmzustand noch einen Störungsmeldezustand an der BMZ erzeugen.

4.2.6 Verlust der Kommunikation

Der Verlust der Fähigkeit der Anlage, eine Meldung eines HF-angebundenen Bestandteils zur BMZ innerhalb der in EN 54-2 bestimmten Zeiten zu übertragen, muss in weniger als 300 s erkannt und in weniger als 100 s angezeigt werden.

Die Prüfung ist nach 8.2.8 durchzuführen.

The Starting Point: EN 54-25



DIN EN 54-25:2009-02
EN 54-25:2008 (D)

Tabelle 5 — Kategorien des Tastverhältnisses

Übertragungszeit/ gesamter Zyklus	Zeit „AN" s	Zeit „AUS" s	Anmerkungen
< 0,1 %	0,72	0,72	z. B. 5 Übertragungen von 0,72 s innerhalb von 1 h
< 1 %	3,6	1,8	z. B. 10 Übertragungen vom 3,6 s innerhalb von 1 h
< 10 %	36	3,6	z. B. 10 Übertragungen von 36 s innerhalb von 1 h
< 100 %	—	—	Typische kontinuierliche Übertragungen, auch solche mit einem Tastverhältnis von > 10 %

WARNUNG — Ein-Kanal-Systeme, die Frequenzen nutzen, bei denen die Zeit „AN" länger als 10 s beträgt, bestehen die Prüfung wahrscheinlich nicht.

8.2.7.2.4 Anforderungen

Die HF-Verbindungen müssen bestimmungsgemäß und wie vorgesehen arbeiten und:

a) keinerlei unbeabsichtigte Störungs- oder Alarmmeldung darf an der Überwachungseinrichtung angezeigt werden, wenn das Störsignal anliegt und

b) alle vorgesehenen Meldungen, z. B. Alarmmeldungen müssen korrekt verarbeitet werden.

8.2.8 Prüfung zur Erkennung bei Verlust der Kommunikation auf einer Verbindung

8.2.8.1 Zweck

Nachweis der Fähigkeit des Empfängers, den Verlust der Kommunikation mit einem Sender in der Anlage zu erkennen.

Die Prüfung muss die Grundfunktion der Anlage nachweisen.

8.2.8.2 Prüfverfahren

Der Hersteller muss ein geeignetes Prüfgerät und ausreichende Angaben zu den Maßnahmen für die Sicherstellung des korrekten und bestimmungsgemäßen Betriebs der HF-Verbindung bereitstellen.

Die Dämpfung zwischen dem zu prüfenden Bestandteil und dessen Partnereinrichtungen darf die Übertragungswege nicht beeinflussen. Bei mehreren zu prüfenden Bestandteilen sind diese ebenso in die Anlage einzubauen.

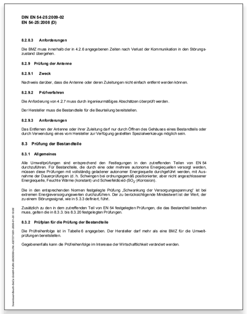
Dann ist zu überprüfen, dass die Überwachungssignale von den Empfängern in Übereinstimmung mit den Herstellerangaben korrekt empfangen werden. Die Übertragung von Überwachungssignalen eines zufällig ausgewählten Bestandteils ist dann für mindestens 300 s zu verhindern, z. B. durch Unterbrechung der Energieversorgung des Senders.

Während der Prüfung ist die vom Hersteller festgelegte maximale Anzahl von Bestandteilen an die Basisstation anzuschließen.

ANMERKUNG Abhängig von der Anlagengestaltung ist es möglich, dass die maximale Anzahl der der BMZ zugewiesenen Bestandteile größer ist als die Anzahl der Bestandteile, die direkt mit der Basisstation verbunden sind.

Die Prüfung ist an einem zufällig ausgewählten Bestandteil durchzuführen und zweimal zu wiederholen.

The Starting Point: EN 54-25



DIN EN 54-25:2009-02
EN 54-25:2008 (D)

8.2.8.3 Anforderungen

Die BMZ muss innerhalb der in 4.2.6 angegebenen Zeiten nach Verlust der Kommunikation in den Störungszustand übergehen.

8.2.9 Prüfung der Antenne

8.2.9.1 Zweck

Nachweis darüber, dass die Antenne oder deren Zuleitungen nicht einfach entfernt werden können.

8.2.9.2 Prüfverfahren

Die Anforderung von 4.2.7 muss durch ingenieurmäßiges Abschätzen überprüft werden.

Der Hersteller muss die Bestandteile für die Beurteilung bereitstellen.

8.2.9.3 Anforderungen

Das Entfernen der Antenne oder ihrer Zuleitung darf nur durch Öffnen des Gehäuses eines Bestandteils oder durch Verwendung eines vom Hersteller zur Verfügung gestellten Spezialwerkzeugs möglich sein.

8.3 Prüfung der Bestandteile

8.3.1 Allgemeines

Alle Umweltprüfungen sind entsprechend den Festlegungen in den zutreffenden Teilen von EN 54 durchzuführen. Für Bestandteile, die durch eine oder mehrere autonome Energiequellen versorgt werden, müssen diese Prüfungen mit vollständig geladener autonomer Energiequelle durchgeführt werden, mit Ausnahme der Dauerprüfungen (d. h. Schwingen bei ordnungsgemäß positionierter, aber nicht angeschlossener Energiequelle, Feuchte Wärme (konstant) und Schwefeldioxid-(SO_2-)Korrosion).

Die in den entsprechenden Normen festgelegte Prüfung „Schwankung der Versorgungsspannung“ ist bei extremen Energieversorgungswerten durchzuführen. Der zu berücksichtigende Mindestwert ist der Wert, der zu einem Störungssignal, wie in 5.3.3 definiert, führt.

Zusätzlich zu den in dem zutreffenden Teil von EN 54 festgelegten Prüfungen, die das Bestandteil bestehen muss, gelten die in 8.3.3. bis 8.3.20 festgelegten Prüfungen.

8.3.2 Prüfplan für die Prüfung der Bestandteile

Die Prüfreihenfolge ist in Tabelle 6 angegeben. Der Hersteller darf mehr als eine BMZ für die Umweltprüfungen bereitstellen.

Gegebenenfalls kann die Prüfreihenfolge im Interesse der Wirtschaftlichkeit verändert werden.

Consolidating Analysis

(R1) The loss of the ability of the system to transmit a signal from a component to the central unit is

- detected in less than 300 seconds and
- displayed at the central unit within 100 seconds thereafter.

(R2) A single alarm event is displayed at the central unit within 10 seconds.

(R3) Two alarm events occurring within 2 seconds of each other are both displayed at the central unit within 10 seconds after their occurrence.

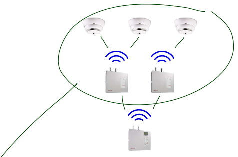
(R4) Out of exactly ten alarms occurring simultaneously,

- the first should be displayed at the central unit within 10 seconds and
- all others within 100 seconds.

(R5) There must be no spurious displays of events at the central unit.

(R6) Requirements (R1) to (R5) must hold as well in the presence of radio interference by other users of the frequency band.
Radio interference by other users of the frequency band is simulated by a jamming device specified in the standard.

Dictionary



(Arenis et al., 2016)

Central Unit: the device which displays warnings and alarms

Component: all devices in the system except for the central unit
(sensors and repeaters)

Slave: a component to be monitored for “ability to transmit”
(sensors and repeaters may be slaves)

Master: a component monitoring slaves
(repeaters and the central unit may be slaves)

Topology: a master/slave relation, each slave has exactly one master

Observables

- Let T be a WFAS topology over the set $C = \{c_0, c_1, \dots, c_n\}$ of components $c_1, \dots, c_n$ and central unit c_0.
- Let $F = \{f_1, \dots, f_m\}$ be a finite set of frequency bands used by the WFAS.

We assume the following observables for T $\quad (0 \leq i \leq n, 1 \leq j \leq m)$:

- $\mathit{RDY} : \{0, 1\}$ – 1 iff the system has been declared ready for use.
- $\mathit{FAIL} : \{\bot, 1, \dots, n\}$ – i iff component c_i is unable to transmit, $\bot$ otherwise.
- $\mathit{DET}_i : \{0, 1\}$ – 1 iff master of component c_i has detected a failure at c_i.
- $\mathit{DISP}_i : \{0, 1\}$ – 1 iff the central unit has displayed an event at component c_i.
- $\mathit{AL}_i : \{0, 1\}$ – 1 iff component c_i has detected an alarm condition.
- $\mathit{JAM}_j : \{0, 1\}$ – 1 iff radio channel f_j is being jammed.

(Environment) Assumptions

$$\Box[\neg(\bigvee_{j,k \in F, j \neq k} \lceil \mathit{JAM}_j \wedge \mathit{JAM}_k \rceil) \wedge \bigwedge_{j \in F} (\lceil \neg\mathit{JAM}_j \rceil ; \lceil \mathit{JAM}_j \rceil ; \lceil \neg\mathit{JAM}_j \rceil \implies \ell \geq 1s) \wedge (\lceil \bigwedge_{j \in F} \neg\mathit{JAM}_j \rceil \implies \ell \leq 1s)] \qquad (\mathrm{Jam}_T)$$

- At most one channel jammed; jam at least 1 s; all free for at most 1 s.

$$\bigwedge_{i \in C} \neg\Diamond(\lceil \mathit{FAIL} = i \rceil ; \lceil \mathit{FAIL} \neq i \rceil) \qquad (\mathrm{FailPers}_T)$$

- Component failures persist.

$$\lceil\rceil \vee \lceil \mathit{FAIL} = \bot \rceil \qquad (\mathrm{NoFail}_T)$$

- No component failure.

$$\lceil\rceil \vee \bigwedge_{i \in C} \lceil \neg \mathit{AL}_i \rceil \qquad (\mathrm{NoAl}_T)$$

- No alarm.

System Requirements: Monitoring

$$\bigwedge_{i \in C} \Box(\lceil \mathit{FAIL} = i \wedge \neg\mathit{DET}_i \rceil \implies \ell \leq 300\mathrm{s}) \qquad (\mathrm{Detect}_T)$$

- Component failure is detected within 300 s.

$$\bigwedge_{i \in C} \Box(\lceil \mathit{DET}_i \wedge \neg\mathit{DISP}_i \rceil \implies \ell \leq 100\mathrm{s}) \qquad (\mathrm{Display}_T)$$

- Detected failures are displayed within 100 s.

$$\bigwedge_{i \in C} \Box(\lceil \mathit{DISP}_i \rceil \implies \lceil \mathit{FAIL} = i \rceil) \qquad (\mathrm{NoSpur}_T)$$

- No spurious display of component failures.

$$\left(\mathrm{FailPers}_T \wedge \mathrm{Jam}_T \wedge \mathrm{NoAl}_T\right) \implies \Box(\lceil \mathit{RDY} \rceil \implies \mathrm{Detect}_T \wedge \mathrm{Display}_T \wedge \mathrm{NoSpur}_T) \qquad (\mathrm{TestMon}_T)$$

System Requirements: Alarm

$$\bigwedge_{i\in C} \lceil \overline{AL_{\{i\}}} \rceil \implies \Box(\lceil AL_i \wedge \neg DISP_i \rceil \implies \ell \leq 10\text{s}), \qquad (\text{Alarm1}_T)$$

- **Exactly one alarm** is **diplayed** **within 10 s**.

$$\bigwedge_{i,k\in C} \lceil \overline{AL_{\{i,k\}}} \rceil \implies \Box[\forall x \bullet (\lceil\rceil \vee (\lceil AL_i \wedge \neg AL_k \rceil \wedge \ell = x \,;\, \lceil AL_i \wedge AL_k \rceil) \wedge \ell \leq 2\text{s} \,;\, true$$
$$\implies \textstyle\int(AL_i \wedge \neg DISP_i) \leq 10\text{s} \wedge (\ell = x \,;\, \int(AL_k \wedge \neg DISP_k) \leq 10\text{s}))] \qquad (\text{Alarm2}_T)$$

- **Exactly two alarms** are **diplayed** **within 10 s**.

within 2s

$$\bigwedge_{i_1,\dots,i_{10}\in C} \lceil \overline{AL_{\{i_1,\dots,i_{10}\}}} \rceil \implies \Box\Big(\big(\lceil AL_i \wedge \neg \bigvee_{i_1,\dots,i_{10}} DISP_i \rceil \implies \ell \cancel{\leq} 10\text{s}\big)$$
$$\wedge \Box\big(\lceil \bigwedge_{i_1,\dots,i_{10}\in C} AL_i \wedge \neg(\bigwedge_{i_1,\dots,i_{10}} DISP_i) \rceil \implies \ell \cancel{\leq} 100\text{s}\big)\Big) \qquad (\text{Alarm10}_T)$$

- Of **exactly ten alarms**, the first is **diplayed** **within 10 s** and all **within 100 s**.

$$(\text{Jam}_T \wedge \text{NoFail}_T) \implies \Box(\lceil RDY \rceil \implies \text{Alarm1}_T \wedge \text{Alarm2}_T \wedge \text{Alarm10}_T) \qquad (\text{TestAl}_T)$$

Content

- **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**

Validating and Clarifying Requirements

Requirements Validation

- **Goal**: **validity** of the **formal representation** wrt. understanding(s) of the requirements (here: at the company).

  Formalisation F is **valid** if and only if

  - for each system scenario S which, in the opinion of the engineers, **does** satisfy the requirements, we have $\mathcal{I}_s \models F$ ($\mathcal{I}_s$: scenario S as evolution), and
  - for each system scenario S which, in the opinion of the engineers, **does not** satisfy the requirements, we have $\mathcal{I}_s \not\models F$.

- **Would be too easy**:

  "Here, this is our proposed formalisation:

$$\bigwedge_{i\in C} \Box(\lceil FAIL = i \wedge \neg DET_i \rceil \implies \ell \leq 300\text{s}) \qquad (\text{Detect}_T)$$

$$\bigwedge_{i\in C} \Box(\lceil DET_i \wedge \neg DISP_i \rceil \implies \ell \leq 100\text{s}) \qquad (\text{Display}_T)$$

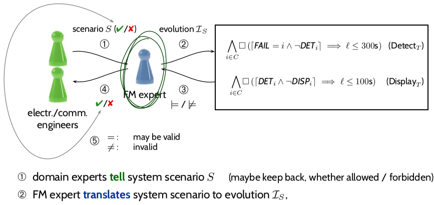
  Please take a look and tell us whether it's valid."

  (Since not every communication partner has an educational background including DC.)

Requirements Validation Cont'd

Two broad directions:

- **Option 1**: teach DC (usually not economic).
- **Option 2**: serve as translator / mediator.



$$\bigwedge_{i\in C} \Box(\lceil FAIL = i \wedge \neg DET_i \rceil \implies \ell \leq 300\text{s}) \quad (\text{Detect}_T)$$

$$\bigwedge_{i\in C} \Box(\lceil DET_i \wedge \neg DISP_i \rceil \implies \ell \leq 100\text{s}) \quad (\text{Display}_T)$$

① domain experts **tell** system scenario S (maybe keep back, whether allowed / forbidden),

② FM expert **translates** system scenario to evolution $\mathcal{I}_S$,

③ FM expert **evaluates** formula on $\mathcal{I}_S$,

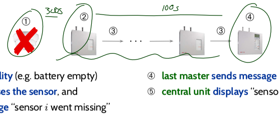
④ FM expert **translates** outcome to "allowed / forbidden by formula",

⑤ compare expected outcome and real outcome.

Example: Detect / Display

(R1) The **loss of the ability** of the system **to transmit** a signal from a component to the central unit is

- **detected** in **less than 300 seconds** and
- **displayed** at the central unit **within 100 seconds** thereafter.



① **sensor** i **loses ability** (e.g. battery empty)

② its **master** m **misses the sensor**, and

③ m **sends a message** "sensor i went missing" to **its master**,

④ **last master sends message** to **central unit**,

⑤ **central unit displays** "sensor i went missing".

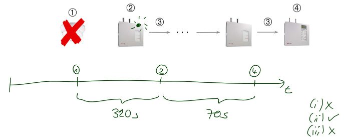
There are (at least) **3 plausible interpretations** of (R1) with repeaters:

(i) "**detection means: central unit knows**": effectively 300 s between 'sensor gone' and 'message at central unit'

(ii) "**detection not really important**": effectively 400 s between 'sensor gone' and 'message at central unit'

(iii) "**detection means: master knows**": then check every 300 s. and have 100 s to transport information to central unit.

Example: Detect / Display (Cont'd)



(i) "**detection means: central unit knows**":
effectively 300 s between 'sensor gone' and 'message at central unit'

(ii) "**detection not really important**":
effectively ~~400 s between 'sensor gone'~~ and 'message at central unit'

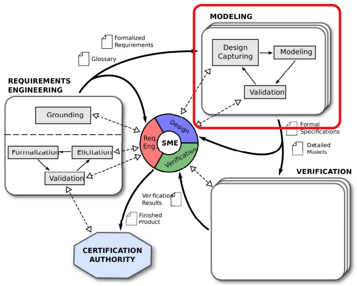
(iii) "**detection means: master knows**":
then check every 300 s. and have 100 s to transport information to central unit.

Content

- **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**

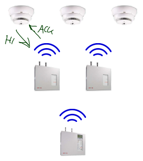
Design Modelling

Formal Behavioural Models

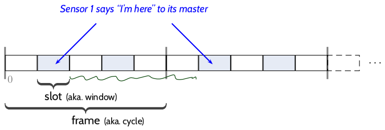


Self-Monitoring

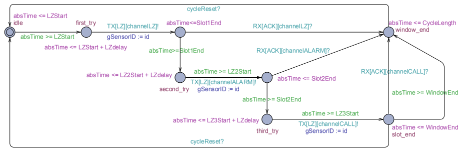
- Periodically, **each sensor** sends a "**hi master, I'm still here**" message to its master.
- If a master misses that message from one of its sensors: report incidence.
- To avoid **message collision**, employ a TDMA (time division multiple access) scheme.



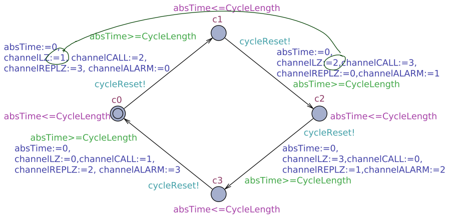
(Arenis et al., 2016)



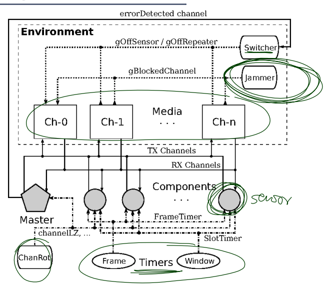
Self-Monitoring: Sensor



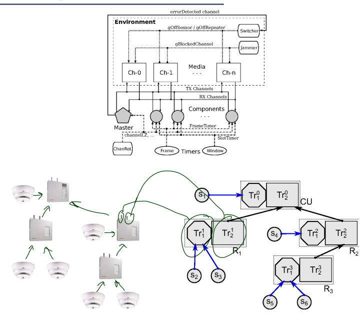
Self-Monitoring: Channel Rotation



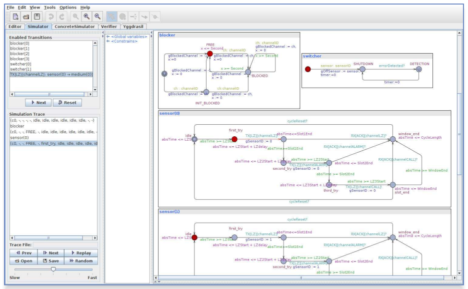
Self-Monitoring: Model Architecture



Self-Monitoring: Model Architecture



Validation



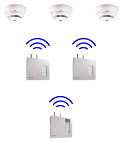
Enabled Transitions:

```
blocker[0]
blocker[1]
blocker[2]
blocker[3]
switcher[0]
switcher[1]
TX[LZ][channelLZ]: sensor(0) → medium(0)[
```

Simulation Trace:

```
(c0, -, -, -, -, idle, idle, idle, idle, idle, idle, -, -)
blocker
(c0, -, -, FREE, -, idle, idle, idle, idle, idle, idle, -
sensor(0)
(c0, -, -, FREE, -, first_try, idle, idle, idle, idle, id
```

Alarm Forwarding

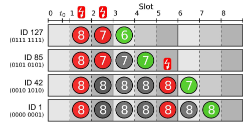


- whenever a sensor **detects indication of fire** (smoke, heat, etc.)
- the sensor **immediately** (next window) sends out an **ALARM message** (the TDMA scheme is only for self-monitoring)
- **that sensor's master** ACK's and forwards the message to its master,
- etc., until the ALARM message reaches the **central unit**.

(Arenis et al., 2016)

- 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):

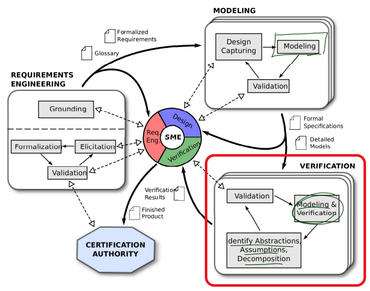


Content

- **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**

Verification

Formal Verification



From DC Formulae 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

References

Arenis, S. F., Westphal, B., Dietsch, D., Muñiz, M., Andisha, A. S., and Podelski, A. (2016). Ready for testing: ensuring conformance to industrial standards through formal verification. *Formal Asp. Comput.*, 28(3):499–527.

Olderog, E.-R. and Dierks, H. (2008). *Real-Time Systems - Formal Specification and Automatic Verification*. Cambridge University Press.