

Real-Time Systems

Lecture 20: Formal Methods for Timed Systems in SME

2018-02-01

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

- 20 - 2018-02-01-man -

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**

- 20 - 2018-02-01-Scontent -

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 total per year ("Jahresbilanzsumme")	$\leq 10 \text{ Mio. €}$ up to 10 Mio. €	$< 50 \text{ Mio. €}$ $\leq 43 \text{ Mio. €}$	$\leq 50 \text{ Mio. €}$ $\leq 43 \text{ Mio. €}$

<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, ...)

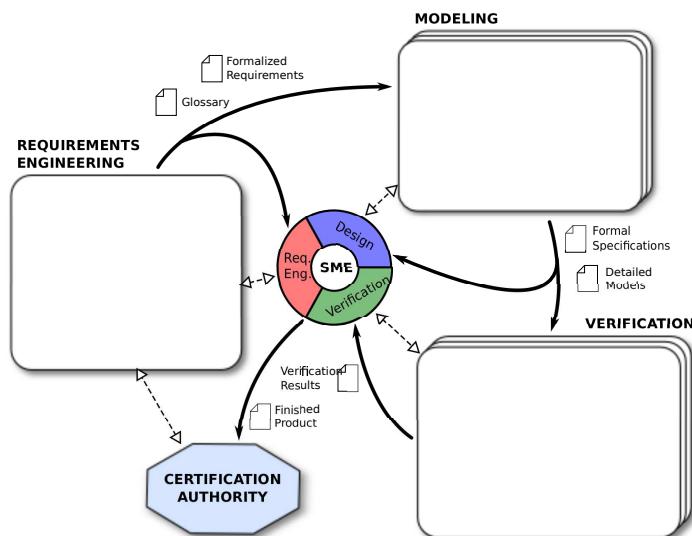
- SME are thus often **hesitant** to implement **changes**, in particular in the **development process**.

Content



Process

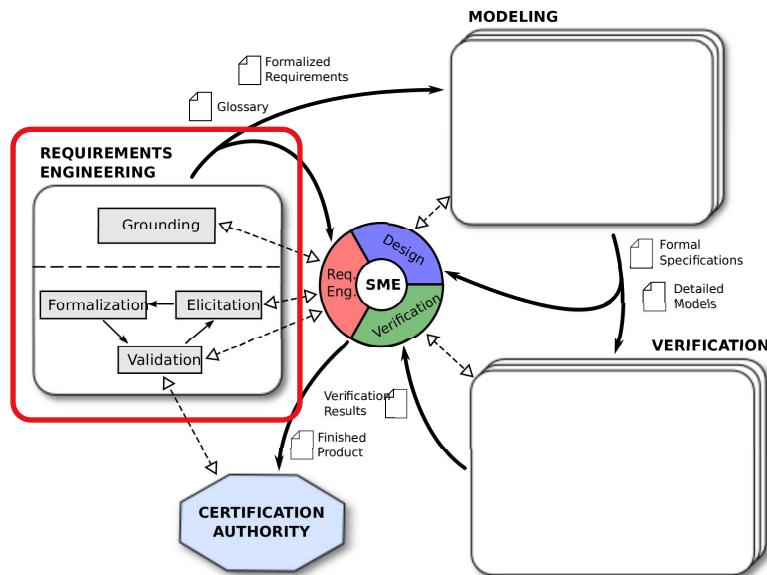
Formal Methods for SME



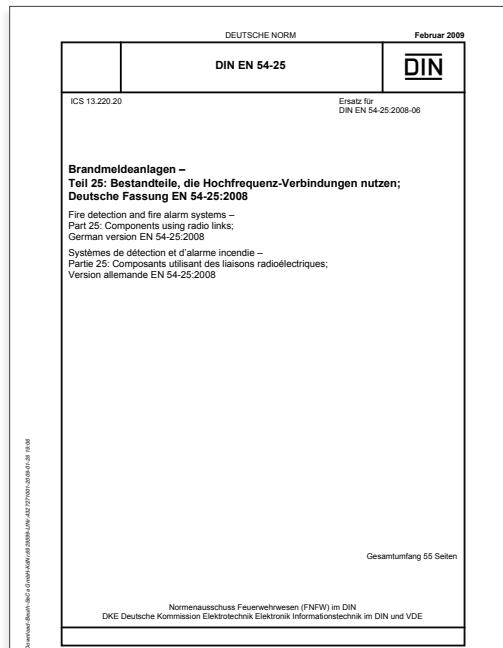
Content

- **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



The Starting Point: EN 54-25



The Starting Point: EN 54-25



<small>DIN EN 54-25:2009-02 EN 54-25:2008 (D)</small>	Inhalt Seite Vorwort 4 Einleitung 6 1 Anwendungsbereich 7 2 Normative Verweisungen 7 3 Begriffe und Abkürzungen 8 3.1 Begriffe 8 3.2 Abkürzungen 10 4 Systemanforderungen 10 4.1 Allgemeines 10 4.2 Hochfrequenzverbindungen 10 4.2.1 Hochfrequenzverbindung 10 4.2.2 Integrität des Alarmsignals 11 4.2.3 Identifikation des HF-angebundenen Bestandteils 11 4.2.4 Identifikation des Empfängers 11 4.2.5 Immunität gegen Störreinflüsse 12 4.2.6 Verlust der Kommunikation 12 4.2.7 Wiederherstellung 13 5 Anforderungen an die Bestandteile 13 5.1 Übereinstimmung 13 5.2 Allgemeines 13 5.2.1 Prüfung der Ausrichtung 13 5.4 Anforderungen an die Umweltprüfung 14 5.4.1 Allgemeines 14 5.4.2 Prüfverfahren 14 5.4.3 Bereitstellung für die Prüfungen 15 6 Dokumentation 15 7 Kennzeichnung 16 8 Prüfungen 16 8.1 Allgemeine Anforderungen 16 8.1.1 Allgemeines 16 8.1.2 Atmosphärische Standardbedingungen 16 8.1.3 Betriebsbedingungen für Prüfungen 16 8.1.4 Minimale Ausrichtung 16 8.1.5 Toleranzen 17 8.1.6 Systemparameter für die Systemprüfungen 17 8.2.1 Prüfung der Immunität gegen Streckendämpfung 17 8.2.2 Prüfung der Integrität der HF-angebundenen Bestandteile 18 8.2.5 Prüfung der Leistungseigenschaften des Empfängers 18 8.2.6 Prüfung der Kompatibilität mit anderen Nutzern des Frequenzbandes 19 8.2.7 Prüfung der Kompatibilität mit anderen Nutzern des gleichen Herstellers 20 8.2.8 Prüfung zur Erkennung bei Verlust der Kommunikation auf einer Verbindung 21 8.2.9 Prüfung der Übertragungsleistung 22 8.3 Prüfung der Bestandteile 22 8.3.1 Allgemeines 22 8.3.2 Prüfung der Lebensdauer der autonomen Energiequelle(n) 22 8.3.3 Überprüfung der Lebensdauer der autonomen Energiequelle(n) 24 8.3.4 Prüfung der Störungsmeldung für den Zustand „schwache Energieversorgung“ 24 8.3.5 Prüfung der Polaritätswechsel 25 8.3.6 Prüfung der Wiederaufmarkierung 26
---	--

- 20 - 2018-02-01 - Seite -

14/52

The Starting Point: EN 54-25



<small>DIN EN 54-25:2009-02 EN 54-25:2008 (D)</small>	DIN EN 54-25:2009-02 EN 54-25:2008 (D) Seite 8.3.7 Prüfung der Exemplarsteigung 26 8.3.8 Prüfung der Verstärkungsparameter 27 8.3.9 Trockene Wärme (in Betrieb) 27 8.3.10 Feuchte Wärme, zyklisch (in Betrieb) 28 8.3.11 Feuchte Wärme, konstant (in Betrieb) 28 8.3.12 Feuchte Wärme, zyklisch (Dauerprüfung) 29 8.3.13 Feuchte Wärme, konstant (Dauerprüfung) 30 8.3.14 Feuchtigkeit, sinusförmig (in Betrieb) 31 8.3.15 SO ₂ -Korrosion (Dauerprüfung) 32 8.3.16 Staub (in Betrieb) 32 8.3.17 Schwingen (in Betrieb) 33 8.3.18 Schwingen, sinusförmig (in Betrieb) 34 8.3.19 Schwingen, sinusförmig (Dauerprüfung) 35 8.3.20 Erdbeben (in Betrieb) 35 Anhang A (normativ) - Prüfkonfiguration für die Verwendung des gegen Hochfrequenzen abgeschirmten Prüfgerätes 37 Anhang B (normativ) Immunität gegen Streckendämpfung (Unterbrechung des Übertragungsweges) 41 Anhang C (informativ) Daten und Berechnung der Lebensdauer autonomer Energiequelle(n) 42 Anhang ZA (informativ) Abschnitte dieser Europäischen Norm, die die Bestimmungen der EG-Bauproduktrennrichtlinie (89/106/EWG) betreffen 44 Literaturhinweise 53
---	--

- 20 - 2018-02-01 - Seite -

14/52

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:

- Funkbeeinträchtigungen aus der eigenen Anlage;
 - Funkbeeinträchtigungen von anderen Nutzern des Spektrums.
- Die folgenden Einflüsse werden hier nicht behandelt:
- zufällige Einflüsse durch elektromagnetische Effekte, da diese in den EMV-Richtlinien behandelt werden (siehe EN 50130-4);
 - 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 Definition 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 Stromungsmitteilzustand an der BMZ erzeugen.

Die Prüfung ist nach 8.2.7 durchzuführen.

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 %	—	—	Yatayette kontinuierliche Übertragungen nach solche mit einem Tastverhältnis von > 10 %.

WARNUNG: Ein-Kanal-Systeme, die Frequenzen nutzen, bei denen die Zeit „AN“ länger als 10 s beträgt, benötigen die Prüfung wahrscheinlich nicht.

8.2.7.2.4 Anforderungen

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

- keinerlei unbedachtige Störungs- oder Alarmsmeldung darf an der Überwachungseinrichtung angezeigt werden, wenn das Störsignal anliegt und
- alle vorgesehenen Meldungen, z. B. Alarmsmeldungen 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 gezieltes Prüfgerät und ausreichende Angaben zu den Maßnahmen für die Sicherstellung des kontinuierlichen und bestmöglichmöglichen Betriebs der HF-Verbindung bereithalten.

Die Dämpfung zwischen dem zu prüfenden Bestandteil und dessen Partneranrichtungen darf die Übertragungswege nicht beeinflussen. Bei mehreren zu prüfenden Bestandteilen sind diese ebenso 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 kann 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 Störungs-
zustand 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 Aus-
nahme der Dauerprüfungen (d. h. Schwingen bei ordnungsgemäß positionierter, aber nicht angeschlossener
Energiequelle) sowie der Prüfung der Feuer- und Säurefestigkeit (CO₂-Korrosion).

Die in den entsprechenden Normen festgelegte Prüfung „Schwankung der Versorgungsspannung“ ist bei
solchen Energieversorgungsarten 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 Prüferfolge ist in Tabelle 6 angegeben. Der Hersteller darf mehr als eine BMZ für die Umwelt-
prüfungen bereitstellen.
Gegebenenfalls kann die Prüferfolge im Interesse der Wirtschaftlichkeit verändert werden.

- 20 - 2018-02-01 - Seite -

14/52

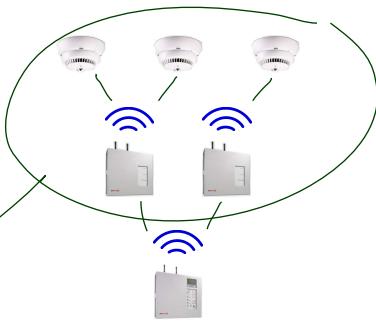
Consolidating Analysis

- (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.

- 20 - 2018-02-01 - Seite -

15/52

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 ($0 \leq i \leq n, 1 \leq j \leq m$):

- $RDY : \{0, 1\} - 1$ iff the system **has been declared ready for use**.
- $FAIL : \{\perp, 1, \dots, n\} - i$ iff component c_i **is unable to transmit**, \perp otherwise.
- $DET_i : \{0, 1\} - 1$ iff **master** of component c_i **has detected a failure** at c_i .
- $DISP_i : \{0, 1\} - 1$ iff the central unit **has displayed an event** at component c_i .
- $AL_i : \{0, 1\} - 1$ iff **component** c_i **has detected** an alarm condition.
- $JAM_j : \{0, 1\} - 1$ iff **radio channel** f_j **is being jammed**.

(Environment) Assumptions

$$\square \left[\neg \left(\bigvee_{j,k \in F, j \neq k} [\text{JAM}_j \wedge \text{JAM}_k] \right) \wedge \right. \\ \left. \bigwedge_{j \in F} (\neg [\text{JAM}_j]; [\text{JAM}_j]; \neg [\text{JAM}_j] \implies \ell \geq 1s) \wedge \left(\bigwedge_{j \in F} \neg [\text{JAM}_j] \implies \ell \leq 1s \right) \right] \quad (\text{Jam}_T)$$

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

$$\bigwedge_{i \in C} \neg \diamond ([\text{FAIL} = i] ; [\text{FAIL} \neq i]) \quad (\text{FailPers}_T)$$

- Component failures persist.

$$[\] \vee [\text{FAIL} = \perp] \quad (\text{NoFail}_T)$$

- No component failure.

$$[\] \vee \bigwedge_{i \in C} \neg [\text{AL}_i] \quad (\text{NoAl}_T)$$

- No alarm.

18/52

- 20 - 2018-02-01 - Se -

System Requirements: Monitoring

$$\bigwedge_{i \in C} \square ([\text{FAIL} = i \wedge \neg \text{DET}_i] \implies \ell \leq 300s) \quad (\text{Detect}_T)$$

- Component failure is detected within 300 s.

$$\bigwedge_{i \in C} \square ([\text{DET}_i \wedge \neg \text{DISP}_i] \implies \ell \leq 100s) \quad (\text{Display}_T)$$

- Detected failures are displayed within 100 s.

$$\bigwedge_{i \in C} \square ([\text{DISP}_i] \implies [\text{FAIL} = i]) \quad (\text{NoSpur}_T)$$

- No spurious display of component failures.

$$\left(\begin{array}{l} \text{FailPers}_T \wedge \text{Jam}_T \wedge \text{NoAl}_T \\ \implies \square ([\text{RDY}] \underbrace{\implies \text{Detect}_T \wedge \text{Display}_T \wedge \text{NoSpur}_T)}_{}) \end{array} \right) \quad (\text{TestMon}_T)$$

- 20 - 2018-02-01 - Se -

19/52

System Requirements: Alarm

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

- Exactly one alarm is displayed within 10 s.

$$\begin{aligned} \bigwedge_{i,k \in C} \lceil \overline{AL_{\{i,k\}}} \rceil &\implies \square [\forall x \bullet (\lceil \cdot \vee (\lceil AL_i \wedge \neg AL_k \rceil \wedge \ell = x ; \lceil AL_i \wedge AL_k \rceil) \wedge \ell \leq 2\text{s} ; true \\ &\implies \lceil AL_i \wedge \neg DISP_i \rceil \leq 10\text{s} \wedge (\ell = x ; \lceil AL_k \wedge \neg DISP_k \rceil \leq 10\text{s})] \end{aligned} \quad (\text{Alarm2}_T)$$

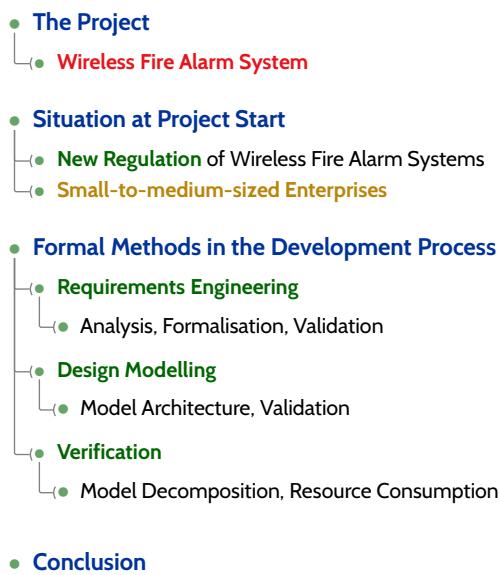
- Exactly two alarms are displayed within 10 s.

$$\begin{aligned} \bigwedge_{i_1, \dots, i_{10} \in C} \lceil \overline{AL_{\{i_1, \dots, i_{10}\}}} \rceil &\implies \square \left(\left(\lceil AL_i \wedge \neg \bigvee_{i_1, \dots, i_{10}} DISP_i \rceil \implies \ell \leq 10\text{s} \right) \right. \\ &\quad \left. \wedge \square \left(\lceil \bigwedge_{i_1, \dots, i_{10} \in C} AL_i \wedge \neg \left(\bigwedge_{i_1, \dots, i_{10}} DISP_i \right) \rceil \implies \ell \leq 100\text{s} \right) \right) \end{aligned} \quad (\text{Alarm10}_T)$$

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

$$\left(\lceil \text{jam}_T \wedge \text{NoFail}_T \rceil \right) \implies \square (\lceil RDY \rceil \implies \text{Alarm1}_T \wedge \text{Alarm2}_T \wedge \text{Alarm10}_T) \quad (\text{TestAl}_T)$$

Content



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:

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

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

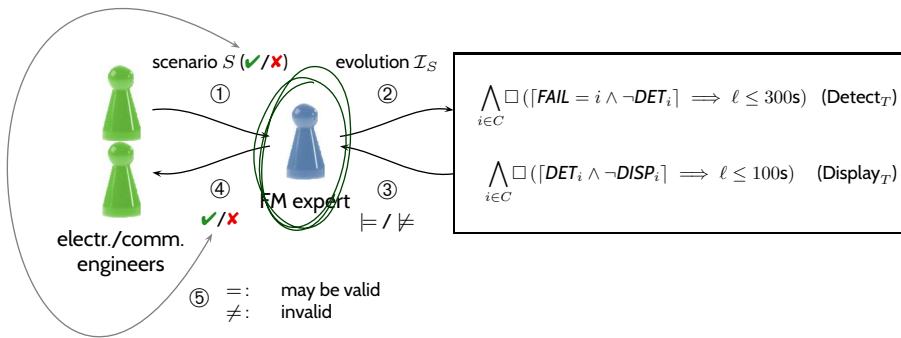
Please take a look and tell us whether it's valid.”

(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.



- 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.

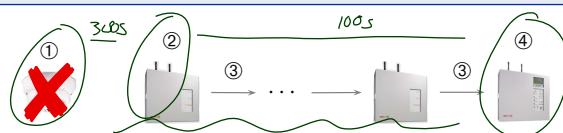
- 20 - 2018-02-01 - Svalid -

24/52

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”.

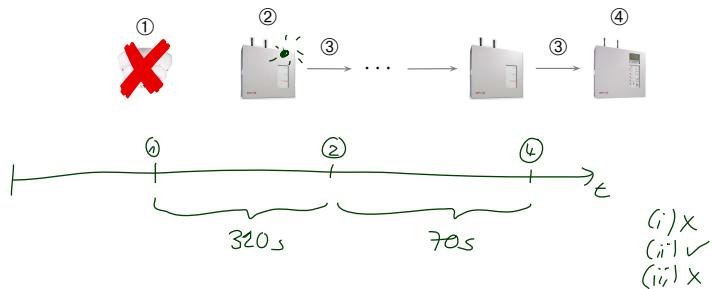
There are (at least) **3 plausible interpretations** of (R1) with repeaters:

- (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.

- 20 - 2018-02-01 - Svalid -

25/52

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’

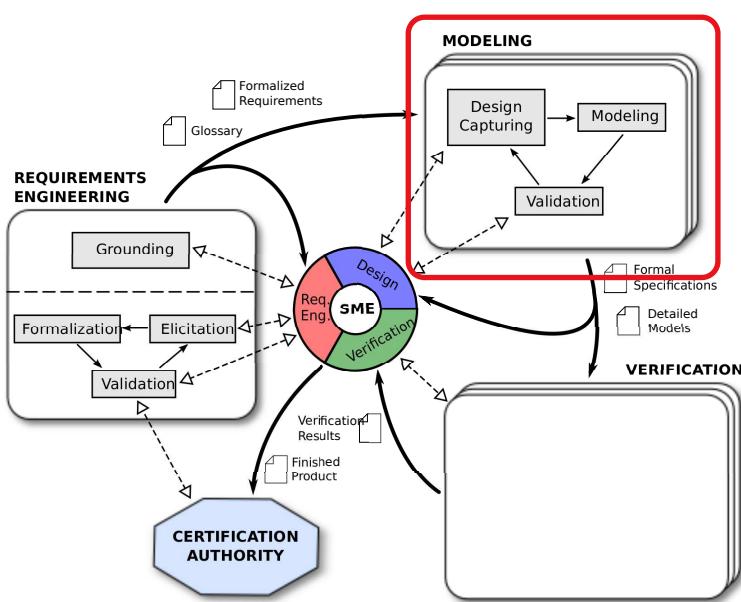
(iii) “**detection means: master knows**”:
then check every 300 s. and have 100 s to transport information to central unit.

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**

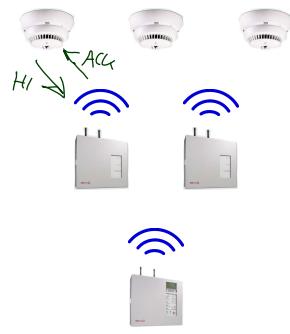
Design Modelling

Formal Behavioural Models



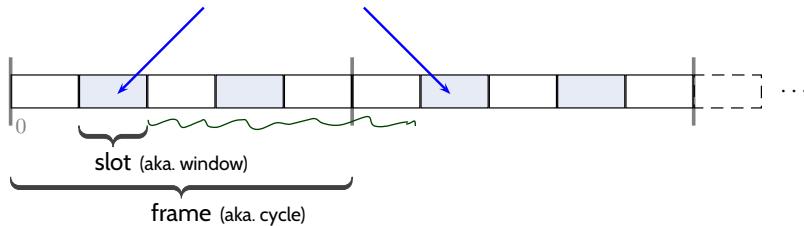
Self-Monitoring

- 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)

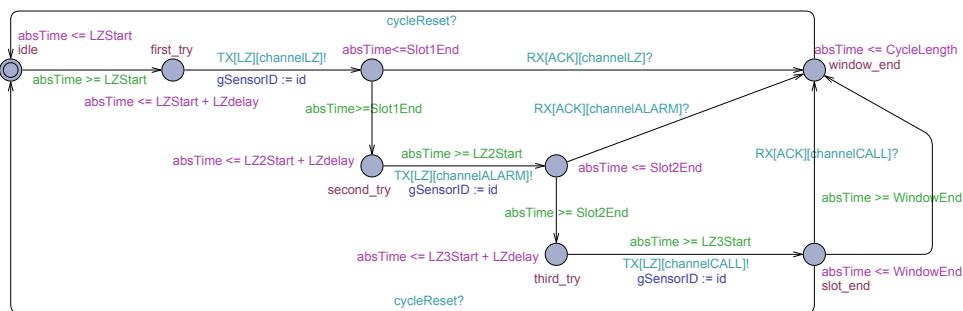
Sensor 1 says “I’m here” to its master



- 20 - 2018-02-01 - Smodel -

30/52

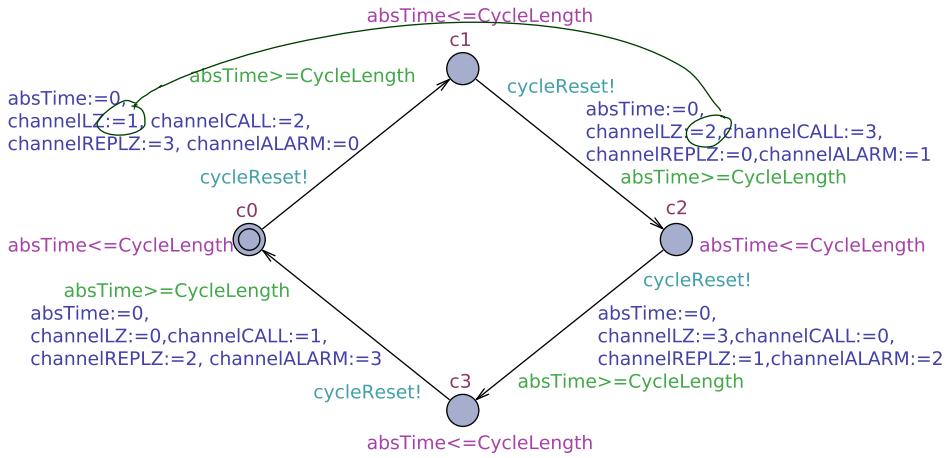
Self-Monitoring: Sensor



- 20 - 2018-02-01 - Smodel -

31/52

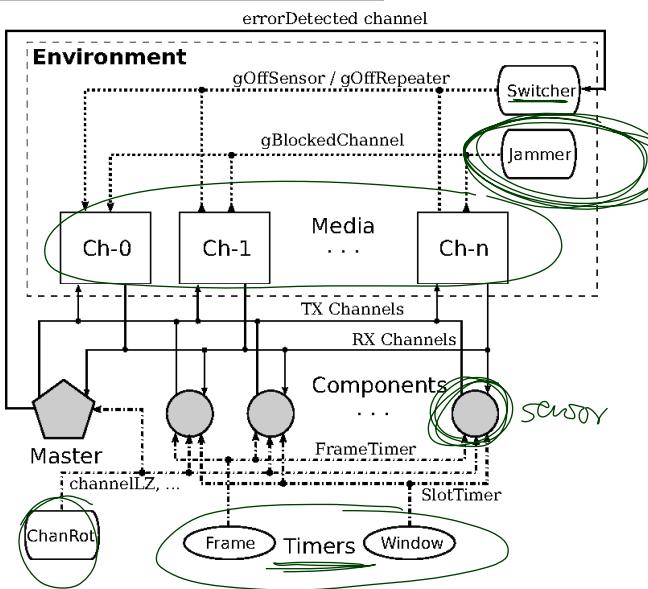
Self-Monitoring: Channel Rotation



- 20 - 2018-02-01 - Smodel -

32/52

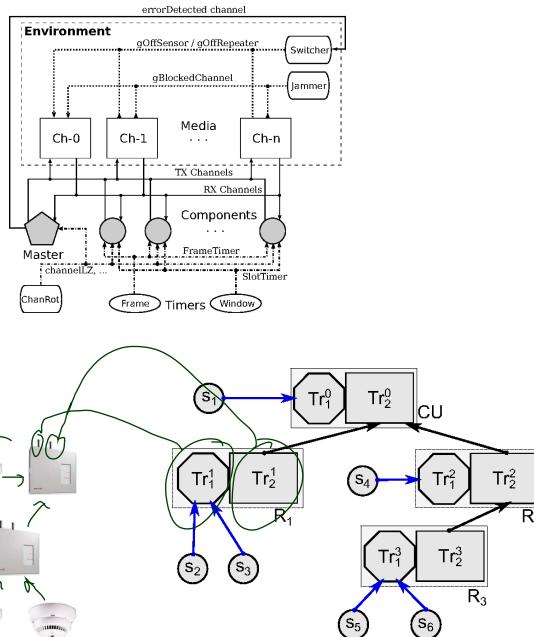
Self-Monitoring: Model Architecture



- 20 - 2018-02-01 - Smodel -

33/52

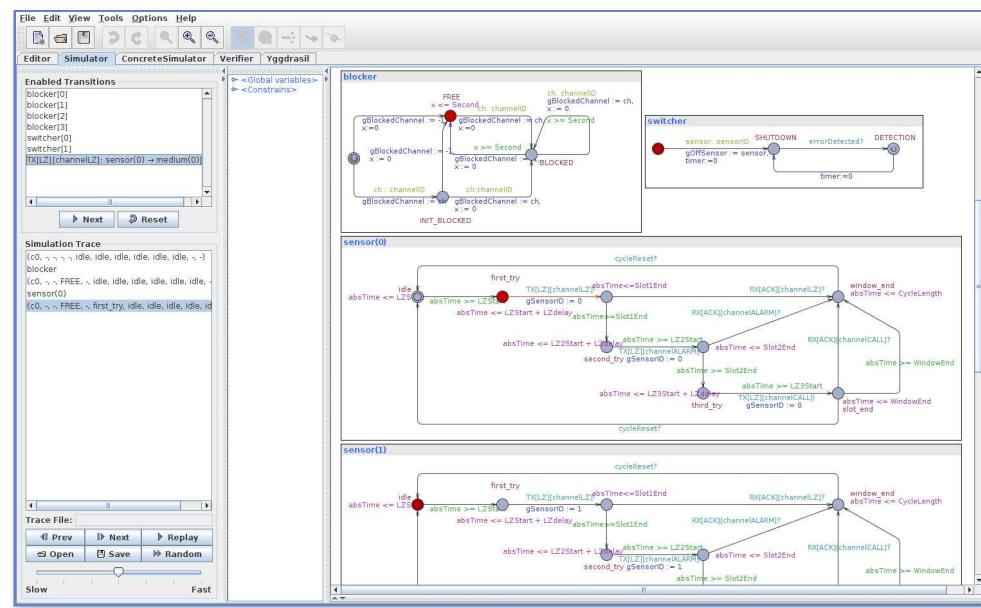
Self-Monitoring: Model Architecture



- 20 - 2018-02-01-Smodel -

33/52

Validation

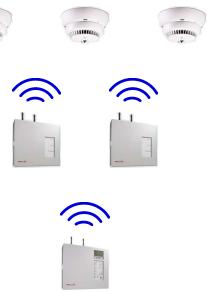


- 20 - 2018-02-01-Smodel -

34/52

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**.

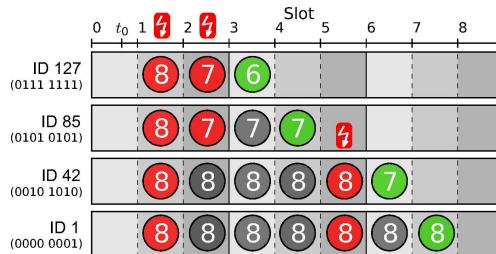


(Arenis et al., 2016)

- What if **two sensors** detect indications of fire **at the same point in time**?

“Message collision” (both send at the same time).

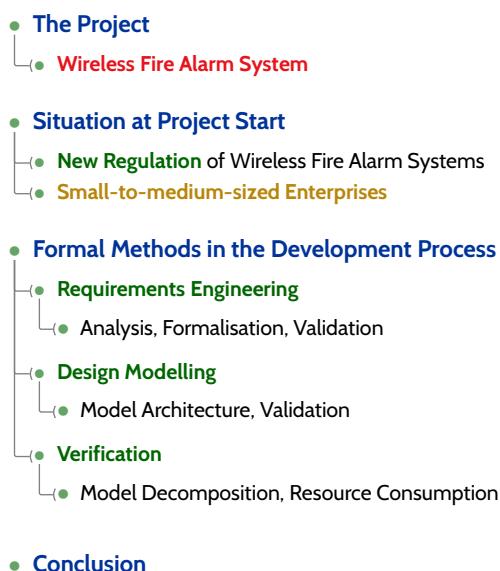
- **Collision resolution** ('tree splitting' protocol):



- 20 - 2018-02-01 - 5model -

35/52

Content

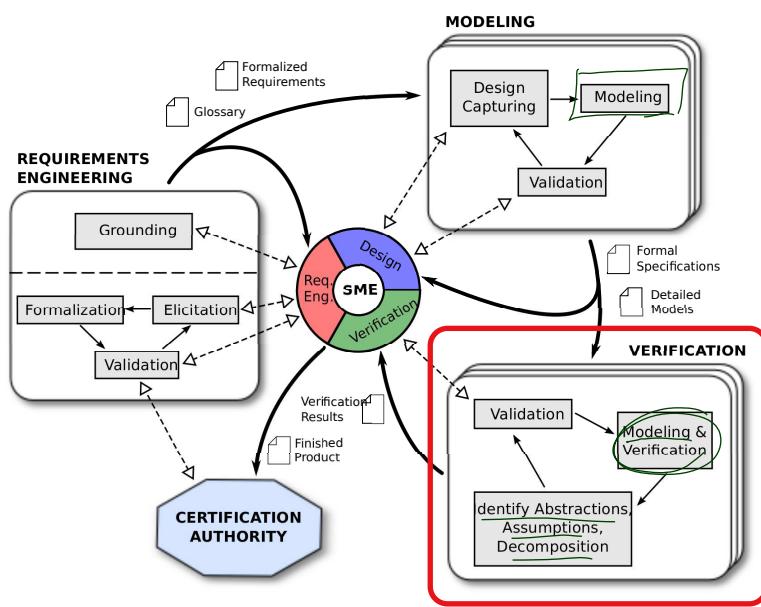


- 20 - 2018-02-01 - 5content -

36/52

Verification

Formal Verification



- **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.