SIEMENS

Linux in Safety-Critical Systems

Experiences in Fire Safety and Security Product Development

Baurzhan Ismagulov <baurzhan.ismagulov@siemens.com>
Siemens Building Technologies

embedded world 2008
Nuremberg, Feb 28 2008

SIEMENS

About Siemens Building Technologies

- 28000 employees in 42 countries
- Activity areas:
  - Security and Surveillance
  - Heating, Ventilation, Air Conditioning
  - Building Automation
  - Fire Safety and Security

SIEMENS

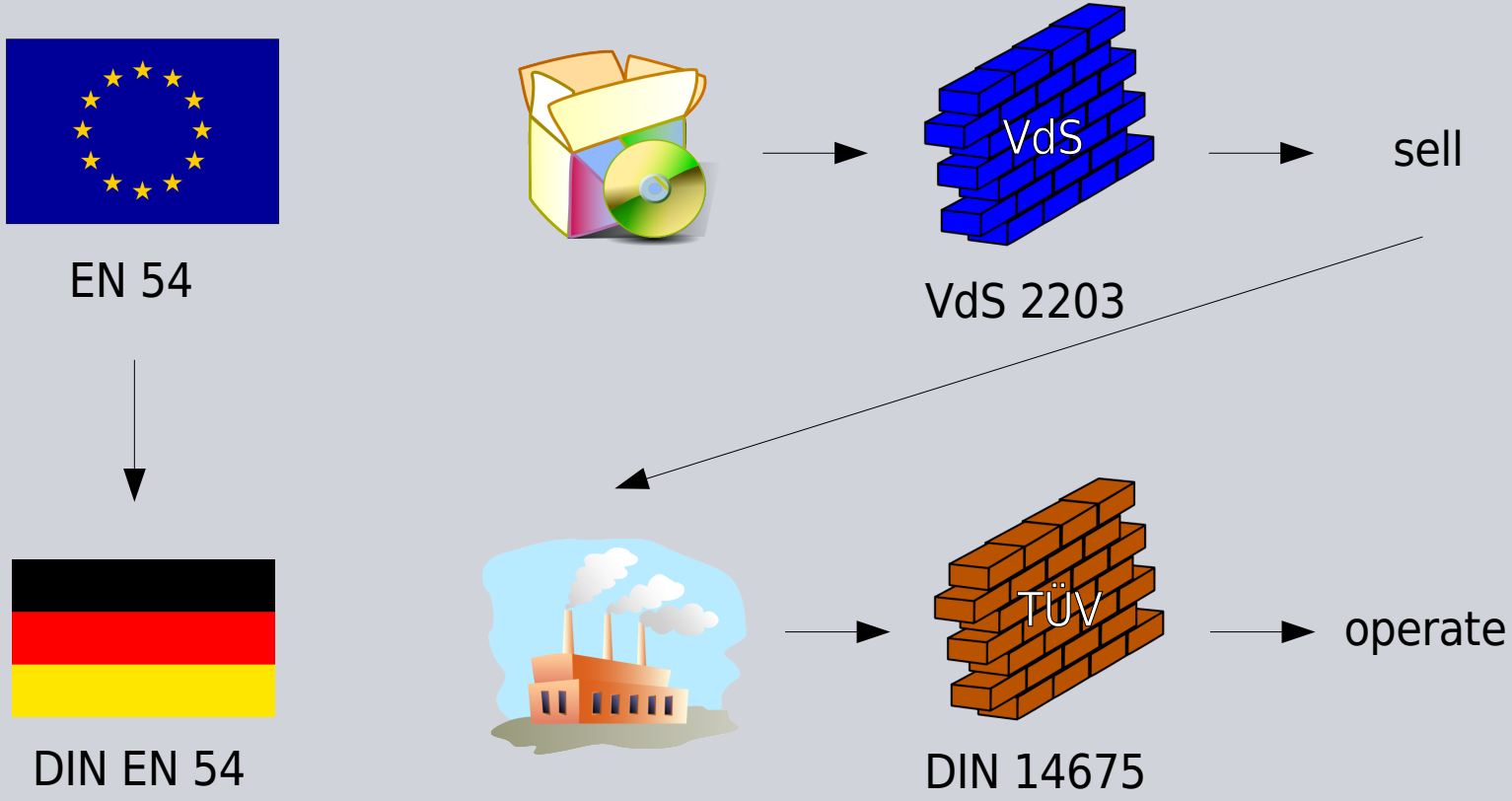
What are Fire Safety and Security Products?

- Basic requirements:
  - Report alarms
  - Report faulty units
  - Enable / disable detectors
  - Detector inspection
- Some further requirements:
  - Scalability → Multiple interconnected panels
  - Information flow → Control panels, fire station wires
  - Reliability, flexibility → Distributed architecture, redundancy
  - Analysis → Logging

FSSP are software-intensive

SIEMENS

Regulations and Stakeholders: An Example



SIEMENS

EN 54

- Defines requirements to FSSP, e.g.:
  - EN 54-1: Introduction
  - EN 54-2: Panels
  - EN 54-4: Power Supplies
  - EN 54-5, 6, 8: Heat Detectors
  - EN 54-7: Smoke Detectors
  - EN 54-9: Testing
  - EN 54-10: Flame Detectors
  - ...
- DIN EN 54: translation with a legal status
- Doesn't specify the certification body
- Doesn't specify the certification procedure

SIEMENS

German Assn. of Property Insurers (VdS)

- VdS is an accredited EN 54 certification body
- Defines:
  - VdS 2344: certification procedure
  - VdS 2203: requirements and testing methods for the FSSP software

SIEMENS

VdS 2344

- Defines the FSSP certification procedure
- Procedure outputs:
  - Conformance certificate: “Conforms with EU norms”
  - Conformance recognition: “Conforms with the norm X”
  - Approval: “Suitable for use in in the field X”
- Describes:
  - Testing
  - Approval
  - Conformance evaluation
  - Warranty
  - Costs
  - Complaints
  - Confidentiality, data protection

SIEMENS

VdS 2203

- Defines requirements and testing methods of the FSSP software
- Looks whether the process is:
  - well-defined
  - repeatable
  - safety-aware
- Tests against EN 54-2, 5, 7
- Methods:
  - Documentation
  - Sample analysis

SIEMENS

VdS 2203 Contents

- Testing criteria examples:
  - Execution flow, memory contents
  - HW and SW interfaces, modularity
  - “Source code listing”
  - Deadlocks
  - Execution monitoring
  - Data checking
- COTS
- Versioning

COTS

- Business necessity:
  - Save development and testing costs
  - Improve quality
  - Reduce time to market
- Siemens software-based deliverables containing COTS:
  - A legacy product line, 1995: 0%
  - A legacy product line, 2006: ~ 15%
  - A new product line, 2007: >> 15%
- VdS 2203:
  - Really COTS?
    - Available to buy by anyone
    - Not outsourced custom development
  - Information about reliability
  - Clearly identified within the product
  - Tested for suitability by the vendor

SIEMENS

Certification Summary

- Certification of Linux-based products possible
- The whole system is certified
  - Not “This Linux distribution is certified for use in fire safety products”
- Does it add value?
  - Costs money and time
- Design for certification:
  - It may affect your design
  - It may affect your inputs and deliverables
- Affects processes:
  - Releases
  - Software updates
- Can be revoked

SIEMENS

Certification, Safety, and Market Economy

- Safety: absense of unacceptable risks
- Risk: damage x probability
- 100% safety doesn't exist
  - Define a desired level of safety
  - Rank by damage, not by probability
- Guarantees will cost you money
- You are liable for errors in your products, not the certification body

Certification does not guarantee safety

SIEMENS

Reading

- Feynman, R.P. “What Do You Care What Other People Think?”
- Schwaber, K. “Agile Project Management with Scrum”
- Kernighan, B.W., Pike, R. “The Practice of Programming”

- EN 54-2 : 1997. “Fire Detection and Fire Alarm Systems. Part 2: Control and Indicating Equipment”.
- VdS 2203 : 2001-03 (02). “VdS-Richtlinien für die Brandschutz- und Sicherungstechnik. Software: Anforderungen und Prüfmethoden”.
- VdS 2344 : 2005-12 (06). “Verfahren für die Prüfung, Anerkennung und Konformitätsbewertung von Geräten, Bauteilen und Systemen der Brandschutz- und Sicherungstechnik”.

- http://en.wikipedia.org/wiki/Test_automation
- http://www.gnu.org/software/dejagnu/

- IEEE Software. http://www.computer.org/software

SIEMENS

Questions?

