Uniform approach of risk communication in distributed IT environments combining safety and security aspects

Jana Fruth and Edgar Nett

Manuela Kanneberg

SAFECOMP 2014, ISSE-WS, Florence, 8th Sep. 2014

- Introduction and motivation
- State of the art
- Uniform approach of risk communication
- Conclusion and future work

Motivation I-IV

Real time systems

(Safety)

IT

(Security)

Heterogeneous technical systems

Requirements to Safety & Security

Two worlds of protection

Safety

Protection of the environment and the system itself against hazards of the system [Sto96]

Examples: safety fences, redundancy of system components

No protection against cyber attacks!

Real time systems

Security

Protection of the system against unauthorised manipulation or retrieval of information [Eck08]

Examples: data redundancy, encryption

Standard information technologies (IT)

Motivation III-IV

Novel hazards and threats:
Potential interdependencies between Safety und Security

[Safe->Sec] Hazards could influence Security

Example:
[Safe] Accidental failure of functions
[Sec] Data loss
Result: Incorrect system functions

Real time systems (Safety)

IT (Security)

Example:
[Sec] Malicious data manipulation
[Safe] Malfunction of robots
Result: Hazard of the environment

[Sec->Safe] Threats could influence Safety

Motivation IV-IV

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG | INF | FACULTY OF COMPUTER SCIENCE

„Risk communication“:

Communication of security and safety risks between humans and industrial automation systems to avoid accidents

Objectives:

- Information of the users of heterogeneous systems on critical system state changes caused by security threats from conventional IT systems
- Guiding of user interactions with the automation system

Main challenges:

1) Dynamic and less predictable behavior of security threats
2) Difficulty in analysis and management of security risks

Approaches:

- Warn the users of potential security threats with impacts on the system’s safety
- Design and realisation of user friendly and comprehensible **risk communication**

→ New concepts are needed!

Overview

- Introduction and motivation
- State of the art
- Uniform approach of risk communication
- Conclusion and future work

State of the art:
Risk communication standards

Real time systems (Safety)

Alarm management standards

IT (Security)

Intrusion detection
standards and guidelines

Limitation:
Selection of standards (DIN, DIN EU, ISO DIN) and recommendations by approved industrial and computer security organisations, which are available free of charge via our library and the Internet

Alarm management systems:

Systems, which detect systematic failures and principles [VDI3699]

Main tasks:

- Safety protection
- Monitoring
- Generation of alarms and warning messages
- Assistance of operators in the process management (analysis of alarms, decision taking of countermeasures)

Human friendly design:

Aim: minimisation of cognitive overload of the operator

- optical-acoustical design principles
- few amount of messages
- guidance through prioritisation, and bundling and suppression of alarms
- designed for standard user

Real time systems (Safety)

Intrusion detection systems:

Systems, which actively monitor computer systems or networks in desktop IT domains to detect attacks and misuse [BSI2002]

Main tasks:

- Security protection
- Monitoring and analysis of log records of unexpected activities and known attacker activities
- Generation of alarms and warning messages

Human friendly design:

Aim: minimisation of cognitive overload of the operator

- optical-acoustical design principles
- few amount of messages
- guidance through prioritisation, and bundling and suppression of alarms
- designed for standard user

IT
(Security)

State of the art: Comparison of risk communication standards

Evaluation criteria:

1. The nature of content (model vs. procedure)
2. Provided phases of the human-automation interaction process (Parasuraman et. al [PSW00])
   - Information acquisition
   - Information analysis
   - Decision selection
   - Action implementation
3. Advantages and properties not covered for the realisation in heterogeneous technical environments

Advantages: Integrated in our new approach

Properties not covered: Motivation for a new risk communication standard

State of the art: Comparison of risk communication standards

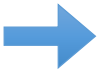
Standard	Content	Advantages	Properties not covered
Industrial Process Control (Safety)			
DIN EN 62541-9 / IEC 62541 (2012) [DIN62541]	Model	1) Formal description of alarms via a holistic **information model** (OPC unified architecture) 2) Exemplary models	1) No providing of information acquisition 2) Only focus on system failures (safety) 3) No user specific model/design examples
NA 102 (Worksheet, 2008) [NA102]	Procedure	1) Providing of all four stages 2) Holistic and interdisciplinary **approach of alarm management design** 3) Optical and acoustical design pattern 4) Examples of practical experiences	Only focus on system failures (safety)
VDI/VDE 3699, Blatt 5 (German Draft, 2013) [VDI3699]	Model (for alarms and messages during **process control with screens**)	Strategies to minimise the cognitive overload of operators	1) No providing of information acquisition and analysis 2) Only focus on system failures (safety) 3) Only optical alarm design

State of the art: Comparison of risk communication standards

Standard	Content	Advantages	Properties not covered
Desktop IT (Security)			
ISO/IEC DIS 27039 (Draft, 2013) [ISO27039]	Procedure	1) Providing of all four stages 2) Holistic procedure of **selection, deployment and operation of IDS** in an organisation	1) Only focus on cyber attacks (security) 2) Only general description of handling of IDS alerts (information and severity of attacks) - no user specific design approaches
BSI - Guideline for introduction of IDS (2002) [BSI2002]	Procedure	1) Providing of all four stages 2) Holistic procedure of **selection, deployment and operation of IDS** in an organisation	1) Only focus on cyber attacks (security) 2) Only general description of alert and incident handling - no user specific design approaches

Existing standards are not sufficient to solve the problems of heterogeneous systems!

New concepts are needed!



Overview

- Introduction and motivation
- State of the art
- Uniform approach of risk communication
- Conclusion and future work

Uniform approach of risk communication

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG | INF | FACULTY OF COMPUTER SCIENCE

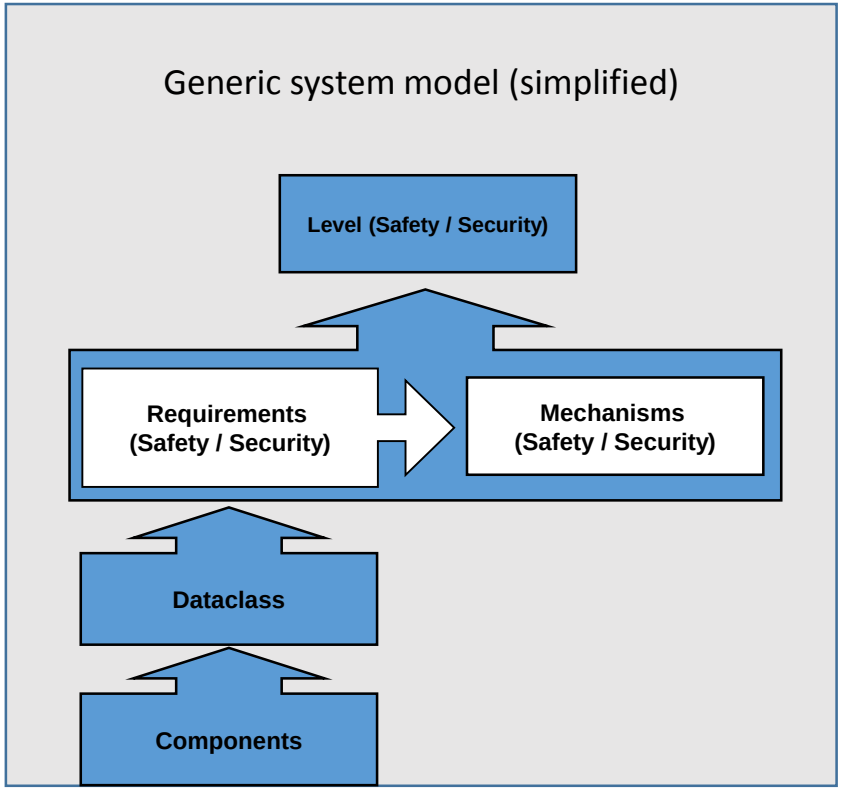
Parts of a new approach for risk communication:

1) Generic system model

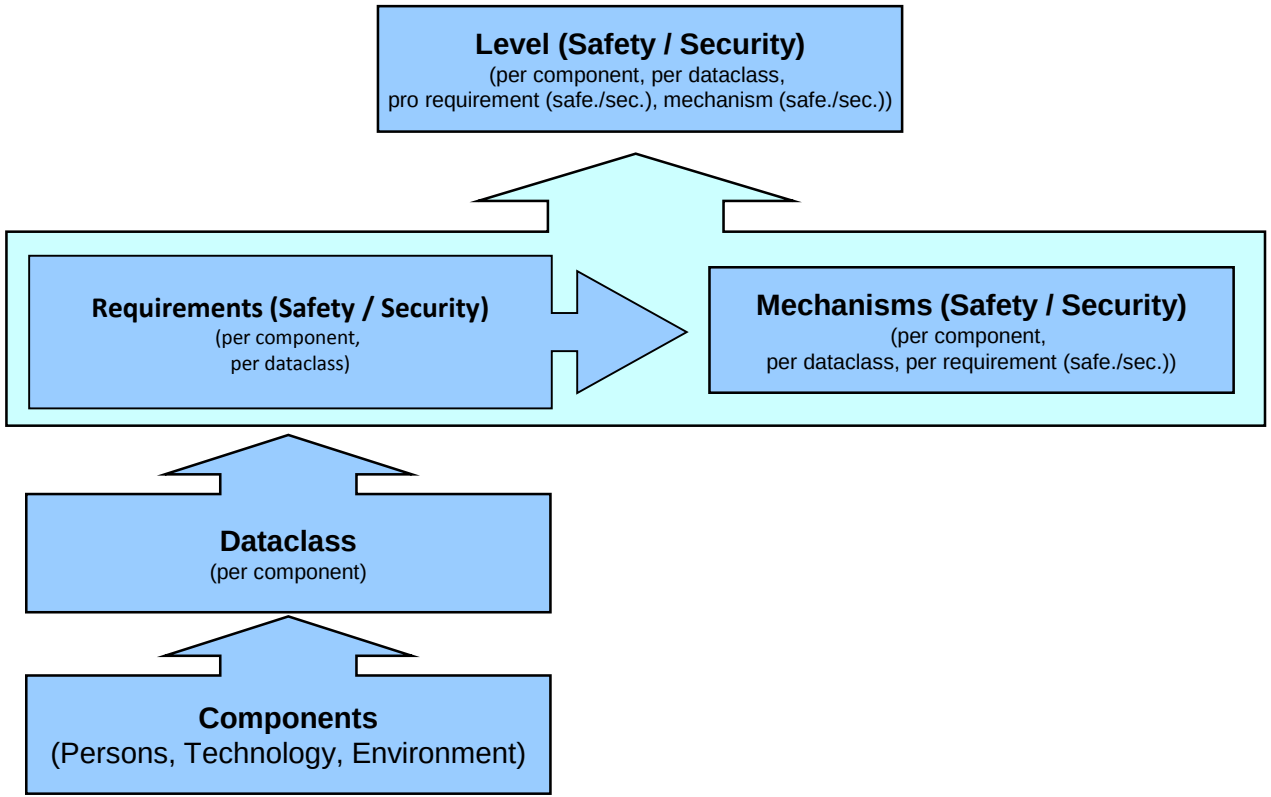
- Including interacting persons and the environment
- Based on an approach for secure data management in embedded systems [FDO+10]

2) User adapted risk communication

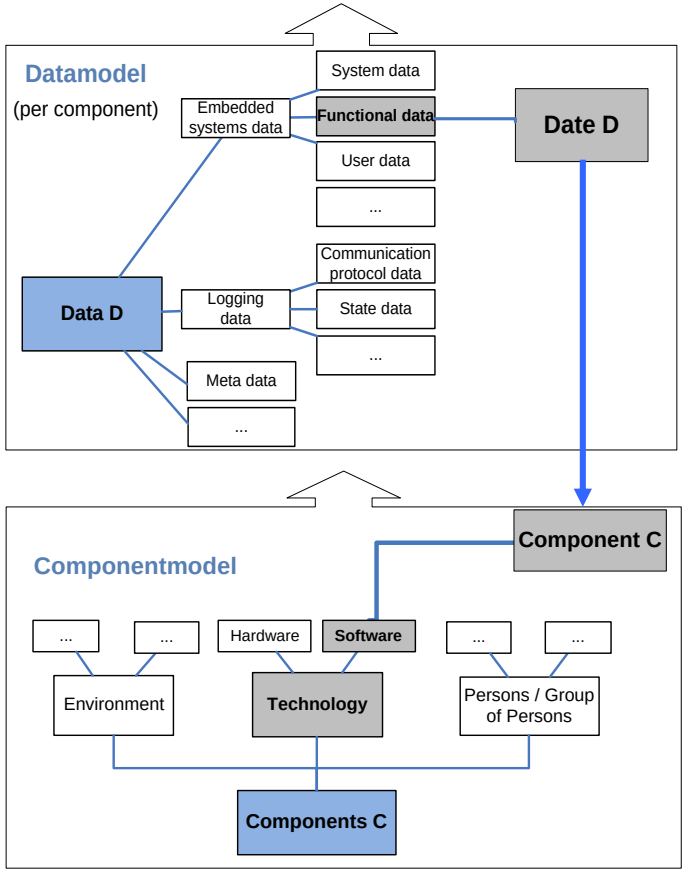
- Based on the phases of the human-automation interaction process (Parasuraman et. al [PSW00])



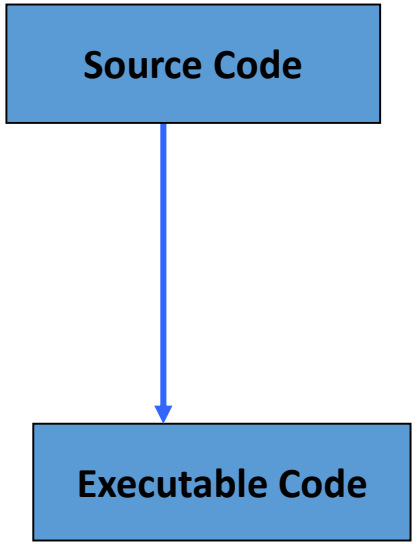
Approach: Generic system model I-III



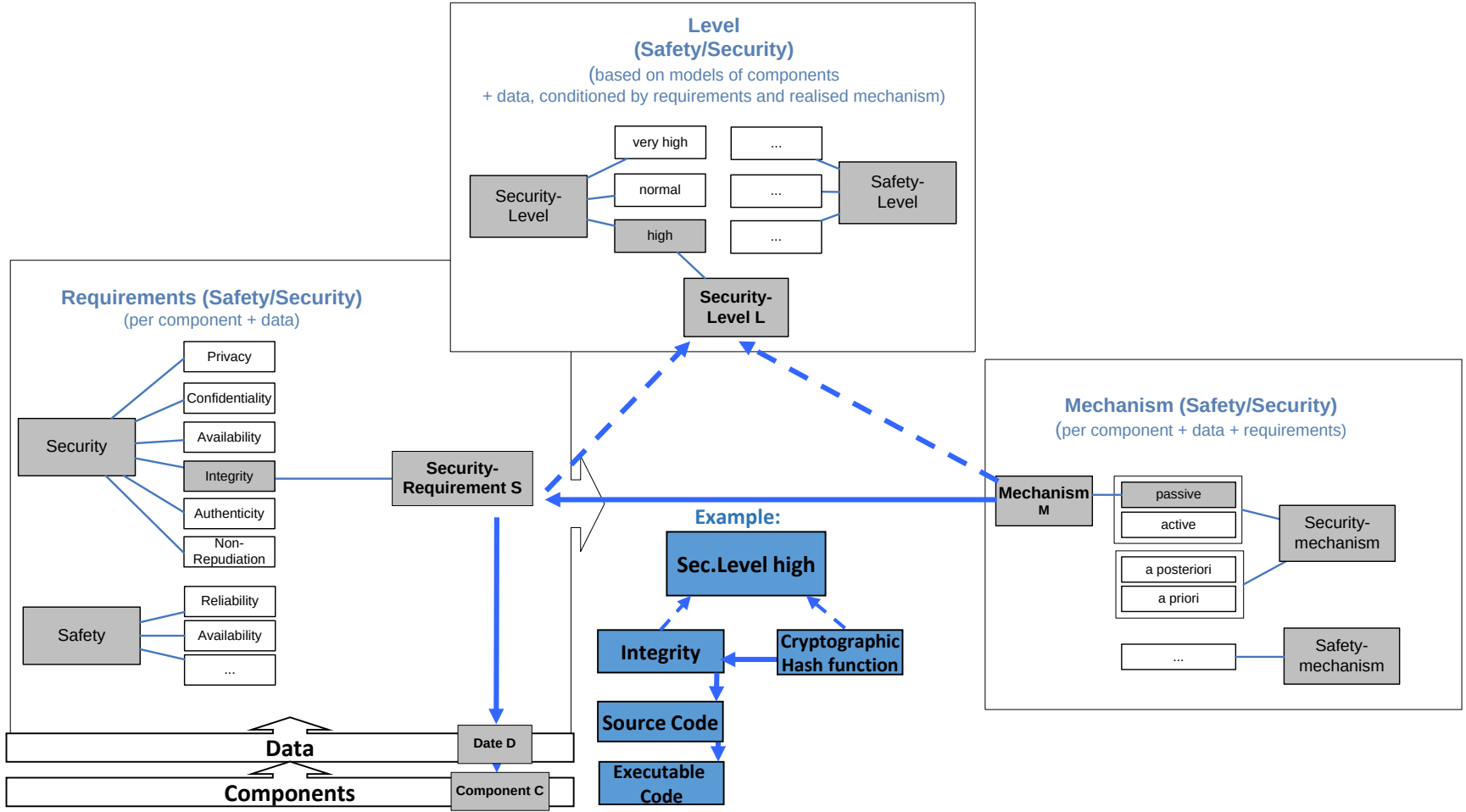
Approach: Generic system model II-III



Example:

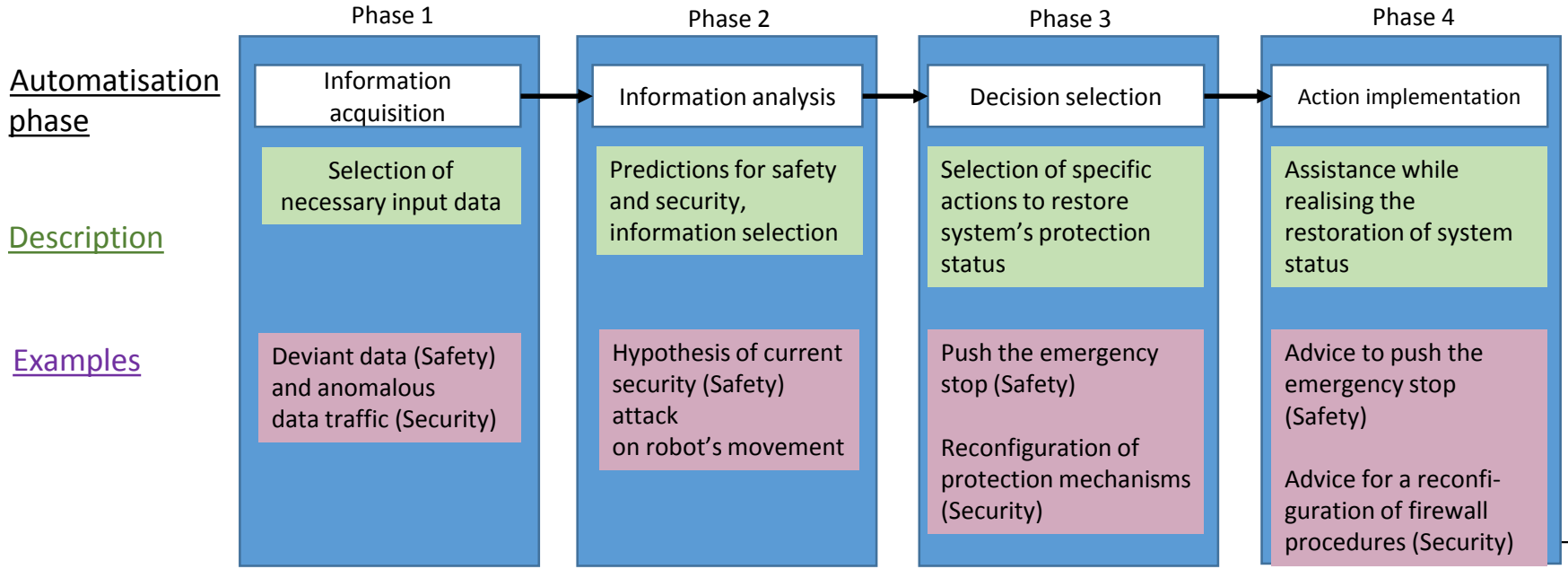


Approach: Generic system model III-III



Approach: User adapted risk communication

- User Assistance in the selection of safety and/or security protection mechanisms in unpredictable situations
- Previous described standards show lack in this area
- Holistic approach is necessary for an adequate risk communication (based on the phases of the human-automation interaction process of Parasuraman et. al [PSW00])



Overview

- Introduction and motivation
- State of the art
- Uniform approach of risk communication
- Conclusion and future work

Conclusion and future work

- Comparison of current safety and security risk communication standards (DIN) using selected evaluation criteria
- Focus on standards of alarm management systems and intrusion detection systems

Results:

  - Only domain-specific solutions
  - Not sufficient to fulfil safety and security requirements of distributed IT environments with safety and security properties

- Introduction of a new model based approach

Future work:

- Research of additional safety and security standards used in general in industrial context
- Extension of analysis of appropriate abilities to cover security and safety requirements in heterogeneous systems
- Specification and evaluation of the holistic risk communication approach
- Practical implementations on selected heterogeneous systems

Thank you for your attention!

Any questions? Please ask: jana.fruth@ovgu.de

References

[**BSI2002**] BSI, ***Introduction to Intrusion Detection Systems - Guideline to introduce IDS***. Tech. Rep. 1.0, BSI - German Federal Oce for Information Security, Con-Secur GmbH (October 2002)

[**DIN62541**] DIN EN 62541-9 / IEC 62541: ***OPC unifed architecture, Part 9: Alarms and conditions*** (June 2013)

[**Eck08**] Eckert, C.: ***IT-Sicherheit: Konzepte - Verfahren - Protokolle***. Oldenbourg Verlag München Wien (2008)

[**FDO+10**] Fruth, J., Dittmann, J., Ortmeier, F., Feigenspan, J.: ***Metadaten-Modell für ein sicheres eingebettetes Datenmanagement***. D-A-CH Security 2010, pp. 359-370 (2010)

[**ISO27039**] ISO/IEC DIS 27039: ***Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)*** (July 2013)

[**NA102**] NA 102: ***Alarm Management***. Tech. rep., NAMUR (October 2008)

[**PSW00**] R. Parasuraman, T.B. Sheridan, C.D. Wickens: ***A model for types and levels of human interaction with automation***, IEEE Trans. Syst. Man Cyber. Part A: Syst. Hum. 30(3), 286–297 (2000)

[**Sto96**] Storey, N.: ***Safety-Critical Computer Systems***. Addison Wesley Longman Limited (1996)

[**VDI3699]** VDI/VDE 3699 Blatt 5: Process control with screens - Alarms/messages (German Draft) (May 2013)