IT Security Protection at Field Level of Industrial Automation Systems

Felix Gutbrodt

International Conference on Embedded Systems and Applications 2007 (ESA '07)
Las Vegas
27. June 2007
Motivation

- Attack against the field level of a chemical plant

\[\text{IT Security Protection at Field Level is imperative}\]
Contents

- IT Security at Field Level
- Protection Concept for the Field Level
- Realization of the Concept
- Summary
The Field Level of Industrial Automation Systems

- Classification of field level in automation pyramid
  - Lowest hierarchy level
  - Connection to technical process

- Tasks of the field level
  - Acquisition and manipulation of process signals
  - Measurement and control within sub-processes

- System elements of the field level
  - Field devices
  - Field buses

- Main constraints of the field level
  - Resource limitation
  - Real-time requirements
Attacks against the Field Level (1)

- Attack against field level IT security
  - Purposeful, not legitimate interaction with field level IT systems

- Interaction requires access to field level
  - Access from higher layers
  - Access by physical connection to field level

→ Here: Protection against attacks with physical connection to field level
Attacks against the Field Level (2)

- Attacks against field buses
  - Eavesdropping
  - Manipulation of content integrity
  - Creation of own messages
  - Manipulation of temporal integrity

- Attacks against field devices
  - Manipulation of functionality

Example: Manipulation of content integrity

- Execution of the attack
  - Connection to CAN field bus
  - Manipulation of content integrity of messages

→ Field level vulnerable
→ Protection required
Contents

- IT Security at Field Level
- Protection Concept for the Field Level
- Realization of the Concept
- Summary
Protection of the Field Level (1)

- Protection functionalities against
  - Manipulation of communication
  - Manipulation of functionality

- Deployment of protection functionalities to field devices

→ Realization of protection functionality that is applicable on field devices?
Decoupling of Protection Functionalities

- Heterogenous technologies at field level
  - Different vulnerabilities
  - Not always all protection functionalities required

→ Selection and deployment of required protection functionalities only
Reduction of Diversity of Protective Mechanisms

- Protective Mechanism: Realize protection functionalities
  - At development time: Agreement on one / few protective mechanisms

→ No negotiations about protective mechanisms required
Modularization of Protective Mechanisms

- Implicit use of comparable operations in different, monolithic protective mechanisms

Multiple use of comparable operations
Multiple Use of Protective Mechanisms

- Avoidance of multiple implementation of protective mechanisms
  - Singular implementation of protective mechanisms
  - Suitable interconnection of protective mechanisms

→ The same protection functionality available while implementing less mechanisms
Selection of Protective Mechanisms

- Protective mechanisms are based upon other protective mechanisms
  → Layer architecture

→ Determination of required protective mechanisms depending on desired protection functionality
Contents

- IT Security at Field Level
- Protection Concept for the Field Level
- Realization of the Concept
- Summary
**Construction of the Layers**

- Abstraction of concrete protective mechanisms

  - Protection Layer 3: Identifier / credentials
    - e.g. MAC

  - Protection Layer 2: Cryptographic hash functions
    - e.g. MD5

  - Protection Layer 1: Encryption
    - e.g. AES

  ➔ Arbitrary protective mechanisms usable

- Selection criteria for protective mechanisms
  - Resource consumption
  - Time determinacy
  - Protection strength
Software Architecture

Realization of the Concept

Protection Functionality | Class of Protective Mechanism | Protective Mechanism (Examples)
---|---|---
Device Functionality | Surveillance / voting | Code Verifier
Temporal Integrity | Temporal marks | Time Stamp
Authorization | Identifier / credentials | DSA
Content Integrity | Cryptographic hash functions | SHA-1
Confidentiality | Encryption | AES
Gliederung

○ IT Security at Field Level

○ Protection Concept for the Field Level

○ Realization of the Concept

○ Summary
Summary

- Protection concept for the field level of industrial automation systems
  - Effective
  - Manipulation proof
- Highly adaptable
- Real-time capable
- Low resource consumption
  - Example (compiled for Renesas M16C/62P)
  - RBAC: 1 kB (ROM) 0.4 ms
  - MD5: 3 kB (ROM) 3.3 ms
  - AES: 5 kB (ROM) 5.8 ms
Thank you for your interest!

E-Mail: felix.gutbrodt@ias.uni-stuttgart.de

www.ias.uni-stuttgart.de