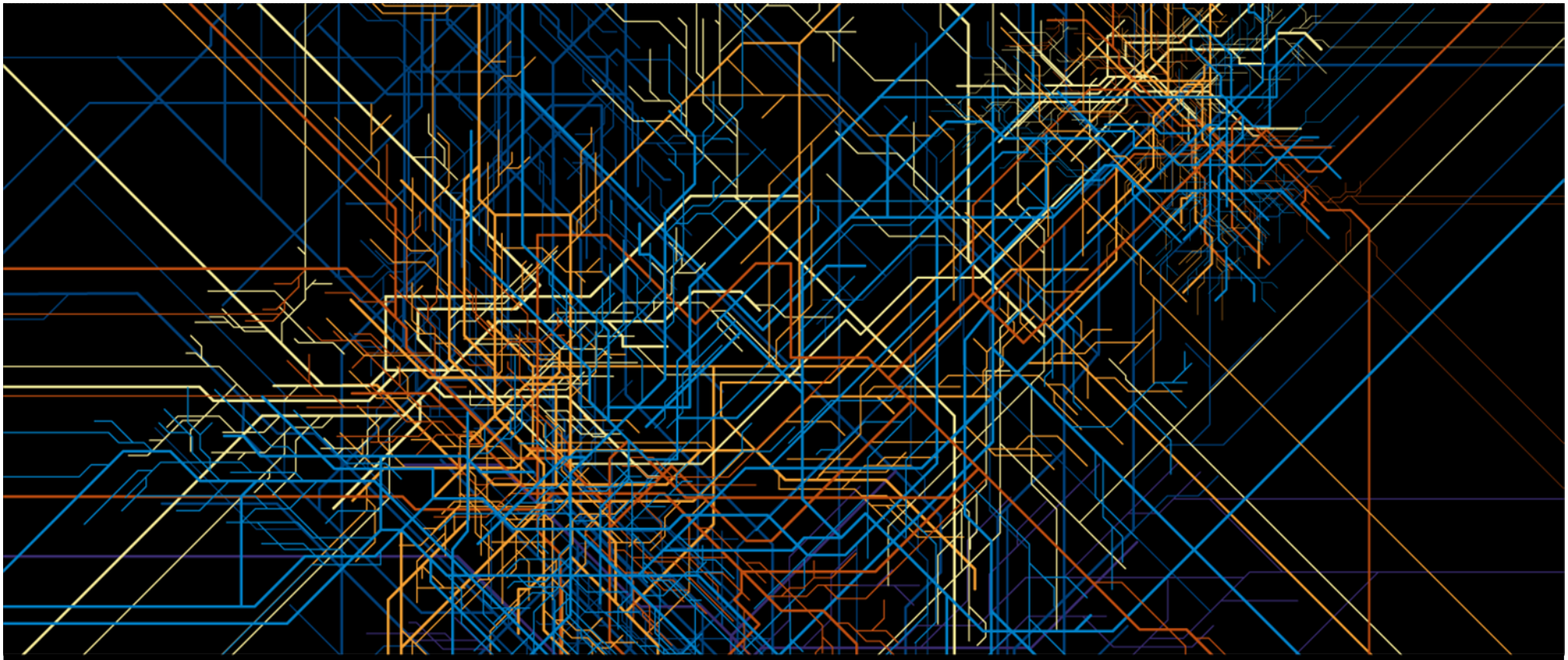


György Kálmán, ABB Corporate Research, 11.11.2013

A tradeoff between security, safety and production continuity

Security Challenges in Safety Instrumented Systems

Security Challenges in SIS

Agenda

- **What is SCADA and DCS**
- **What is a Safety Instrumented System**
  - History
  - Current solutions
  - Challenges and development directions
- **Time scales of automation tasks**
  - Process control security
  - Automation and electric systems
- **Security threats for SIS**
  - Insider threats
  - External threats
- **Production continuity**
  - Tradeoff between safety and security
  - Usable security
  - Technical limits
- **Security and safety in parallel operation**
  - Fail-safe paradigm
  - Fail-operational paradigm
- **State of the Art security solutions**

Security Challenges in SIS

Overview – automation systems - SCADA

- **Supervisory Control and Data Acquisition**
  - Remote control and monitor automation systems
  - Typically low bitrate (this is changing)
  - Large systems both in area and number of devices
  - Access to systems through WAN connections
  - Typical grace time in the seconds range

- **Typical examples:**
  - Power grid or any other public service like water, wastewater, traffic lights
  - Oil and gas pipelines
  - Remote oil production installations

Security Challenges in SIS

Overview – automation systems - DCS

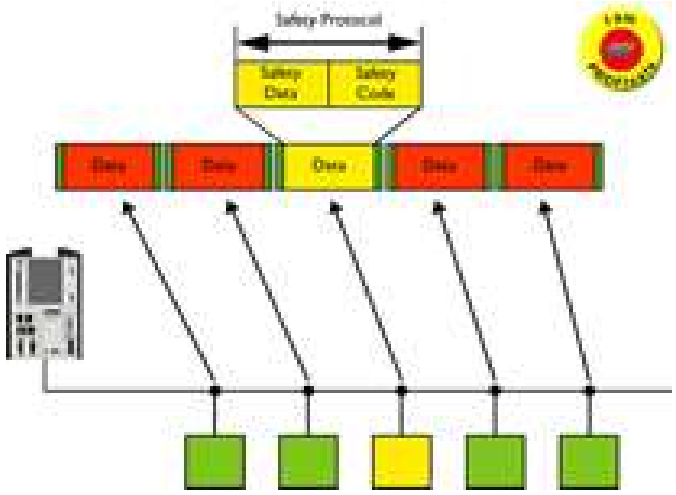
- **Distributed Control System**
  - Local control of automation tasks
  - Typically LAN, using uplink towards Enterprise Resource Planning
  - Covers a smaller geographic area
  - Control of the process of manufacturing task
  - Grace time depends on the actual task
- **Safety**
  - Safety systems are typically placed on this level

- **Typical examples:**
  - Automation system inside a car plant
  - Oil refineries
  - Ships

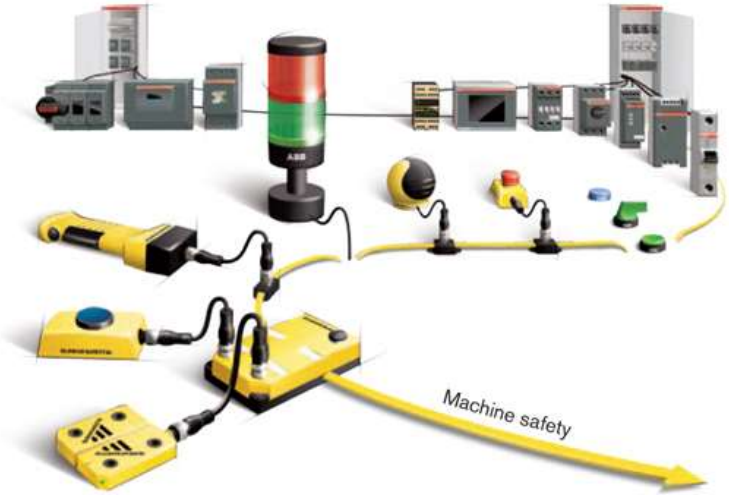
Security Challenges in SIS

Safety Instrumented Systems

- **Goal**
  - Ensures that if an operational problem occours, the system is taken into a safe state to avoid health, safety and environmental damage
- **Current state of the art**
  - Integrated safety systems
  - Shared communication
  - Special diagnostics
  - Leaky-bucket style operation

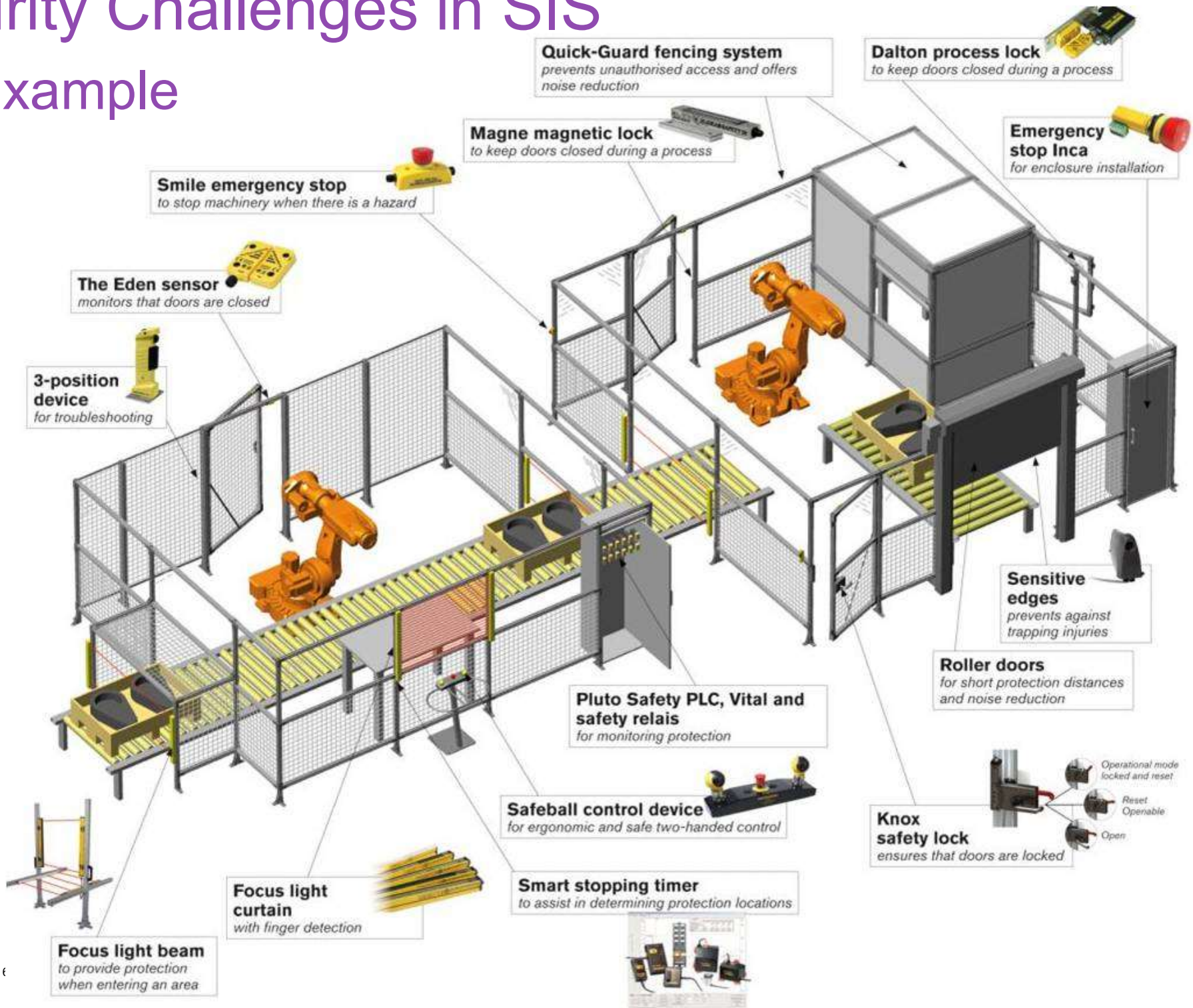


- **Integrity levels**
  - Safety Integrity Level 1-4
  - SIL 3: extensive diagnostics, heterogenous computation paths
  - SIL 4: SIL3+majority voting+more
- **Current development**
  - Model-based design
  - Automatic diagnostics generation
- **No direct communication requirement!**
- **Not tamper proof or sabotage-protected!**



Security Challenges in SIS

SIS Example

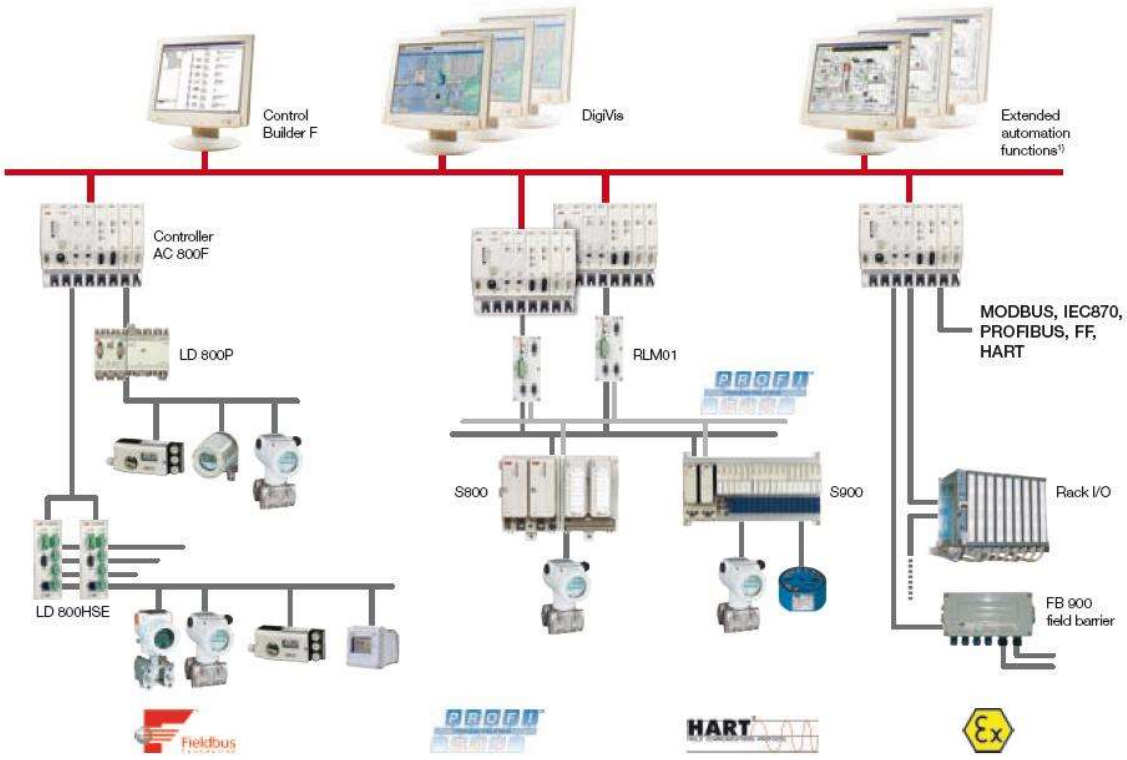


Security Challenges in SIS

Current security measures

- **History**
  - Isolated islands
- **Current state of the art**
  - Shared communication, not only changing to packet-switched, but also using public networks
  - IP networking, Ethernet LANs
  - Firewalls and network segmentation
  - Integration into higher level systems e.g. IT management, ERP
  - Cryptographic functions on controllers and above
- **Perimeter defense**
  - Firewall, IPS, DMZ
- **Internal security**
  - Firewall, IDS, DMZ
  - Monitoring
  - Active scanning

- **Evolution**
  - Security to the field level
  - Evaluation of encryption/authentication of communication
- **Quality of Service?**



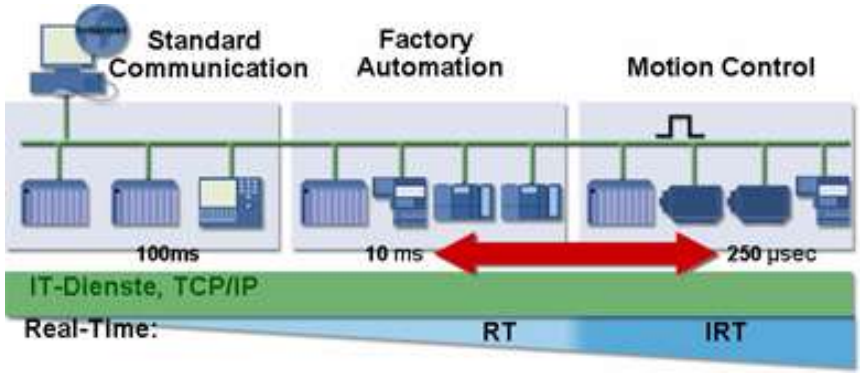
Security Challenges in SIS

Security with respect to Quality of Service

- **SCADA**
  - Low frequency operation
  - Optimized communication
  - Grace times and typical usage allows the inclusion of security measures without violating the service quality

- **DCS**
  - In Process control, a majority of applications are expected to accept a minor delay due to cryptographic functions or other security measures
  - In motion control or bar protection, encryption is currently less feasible, authentication using HMAC is accepted but not widely used

- **Industrial systems are interested in authenticity-integrity-confidentiality**



Security Challenges in SIS

Insider and external threats

- **Employees**
  - Accidental or conscious acts
  - User credentials
  - Special knowledge
  - Non-compliance: messaging, P2P, video players, games on DCS workstations
- **Access**
  - Physical access to devices
    - Social engineering
    - Insuffcient protection
  - Network access
  - Logical access to devices
    - *Security through obscurity*
  - Device tampering
  - Remote (unmanned) sites are backdoors to the control system
  - Devices can be flashed on site
  - Wireless

- **Mitigation**
  - Access control
  - Logging
  - Segmentation
  - HR + education
  - Deploy modern security solutions
  - Device development with security in mind

Security Challenges in SIS

Security, Safety and Production

- **Tradeoff**
  - Compare DCS and IT operation
  - Safety functions need to operate also if the system is compromised
  - Production continuity vs. sensitivity

- **Philosophical problems**
  - Add 5 kg of security
    - Add crypto or authenticaion without knowledge of the undelying system
    - Unreacheable goals
  - Whole picture, including life cycle
  - Facing IT security threats by DCS operators
  - Authenticity-Integrity-Confidentiality vs. Confidentiality-Integrity-Authenticity
  - Low entropy on SCADA data
  - Whitelist can work better in industry, other, non-scalable solutions can be relevant
  - Default usernames, passwords, IP addresses

- **Problems contd.**
  - No patching, 10 year old OS-es can be present
  - No personal authentication
  - As-built analysis

- **Safety function operation**

Security Challenges in SIS

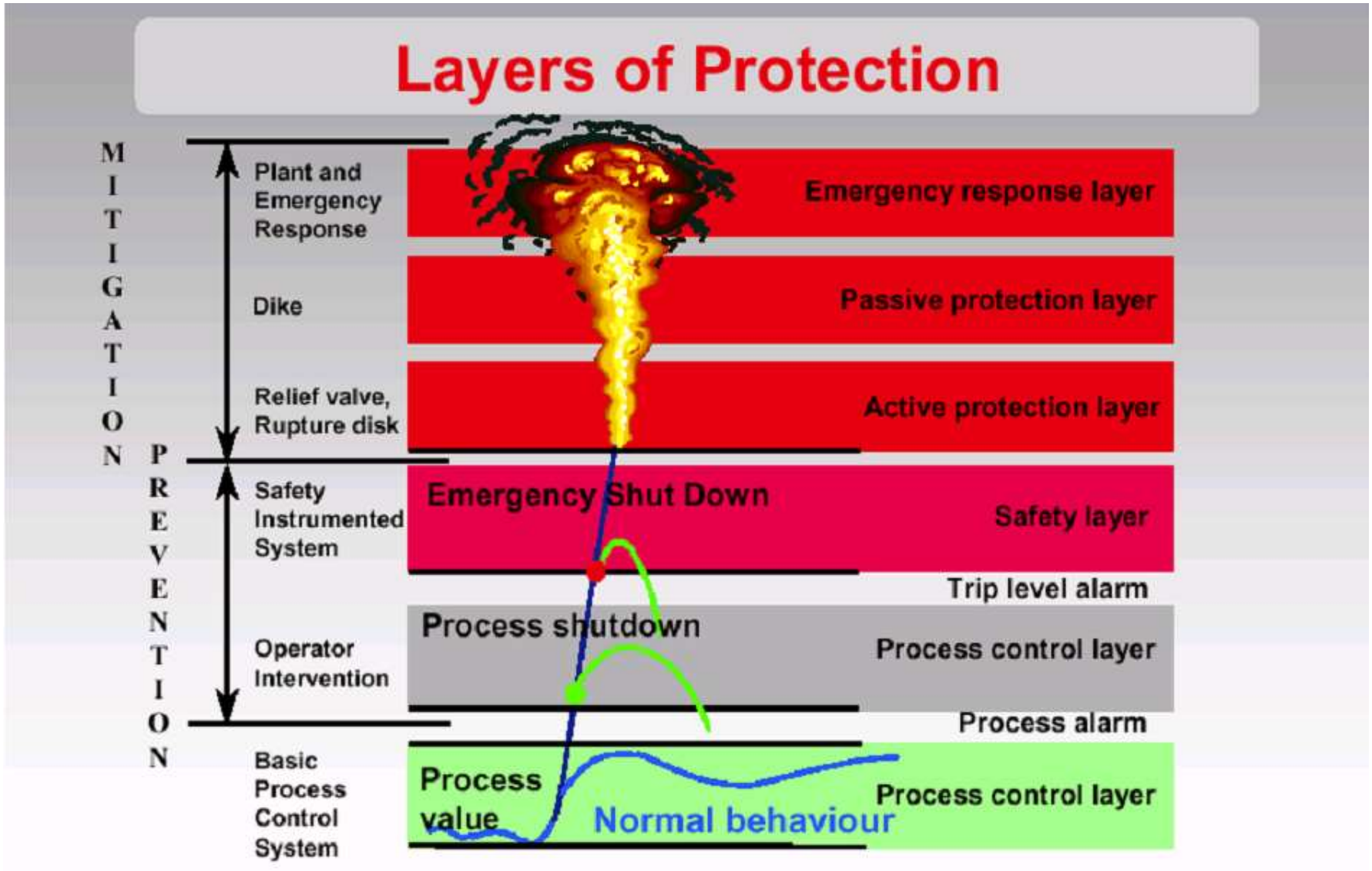
Security and Safety

- **Reason**
  - Connected because security threats are resulting in safety threats, which have to be mitigated
  - Different fields but approaching similar problems
  - The process behind is completely different: safety deals with a static statistical process, while security problems are the result of an active, changing process
- **Security**
  - Stopping somebody to do something to avoid damage
- **Safety**
  - Even if something has happened, avoid or limit damage

- **Cyber-physical interactions**
  - IT security is not covering this field
  - Safety is focusing on the physical interactions
  - Safety is using extensive diagnostics to check itself
  - Timescale of protection and data validity
- **Security of safety diagnostics**
  - Device tamper resistance
  - Predefined vectors
  - Predefined, internal expected results
  - Basic safety function is standalone
  - Pairing of devices (e.g. drive with motor)

Security Challenges in SIS

Security and Safety



- From: The Rocky Relationship Between Safety and Security

Security Challenges in SIS

Security and Safety – Fail reaction

- **Fail-safe**
  - This is the approach what we use in security
  - In case of a breach detection, take down the interface to limit the damage (e.g. refinery or train)
  - Lockout of user if too many bad password tries (not acceptable for automation)
  - Start virusscan
- **Industrial environment**
  - QoS must be kept
  - Safety function must stay intact
  - If security measures are not able to confine the intrusion, safety is expected to provide a secondary protection layer and trap

- **Fail-operational**
  - Keep operation intact (e.g power grid, plane)
  - Confine damage
  - Check if performace indicators are still acceptable and avoid safety trap
- **Dependability and safety**
  - An industrial system is expected to be operational
  - Production interruption has direct physical implications
  - Retrofit of old installations

Security Challenges in SIS

State of the Art

- **Controller level**
  - Industrial firewalls
  - Network interface flood protection
  - Tamper resistant hardware
  - Firmware protection
  - Internal diagnostic
- **Fieldbus level**
  - Message authentication
  - E.g. IEC 61850 non-routeable with HMAC
- **Control network level**
  - Segmentation
  - Message authentication
  - Encryption, PKI
- **Servers and workstations**
  - IT practices are relevant
  - PKI
  - Office software and solutions

- **SCADA (WAN)**
  - VPN
  - Firewalling
  - Strict access control and logging

Security Challenges in SIS

Recommended articles

- Bowen et al.: *Designing Host and Network Sensors to Mitigate the Insider Threat,* IEEE Security and Privacy, Vol.7, number 6, 2009
- Giusebbe Buja, Roberto Menis: *Dependability and Functional Safety*, IEEE Industrial Electronics, Vol.6, Nr. 3, 2012
- Markus Brandle, Martin Naedele: *Security for Process Control Systems, An Overview*, IEEE Security and Privacy, Vol. 6, Nr. 6, 2008

- ISA/IEC 62443-2-1 - Industrial automation and control systems security management system

- Operations and Security from Emerson:
- http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Whitepapers/WP_Operations_Security.pdf
- The Rocky Relationship Between Safety and Security from ABB:
- http://www05.abb.com/global/scot/scot296.nsf/veritydisplay/3e234b767729aaa0c1257aa60064b129/$file/3BUS095673_en_Whitepaper_-_The__Rocky_Relationship_between_Safety_and_Security.pdf

- Stuxnet, Boden wastewater incident in Queensland, Australia.