Functional Safety and Cyber Security

Pete Brown
Safety & Security Officer
PI-UK

Setting the Scene

- Functional Safety requires ‘Security’
- Consider just ‘Cyber Security’ for FS
- Therefore ‘Industrial Control Systems’ (ICS)
- Physical security
- Full ‘defence in depth’
- Safety ‘lifecycle’ not Security ‘lifecycle’
- My personal view
- Discussion point for a way forward

Safety Vs Security

- Independent domains
- Little interaction
- Convergence of technologies
- Common infrastructure
- Conflicting responsibilities
- Engineering Vs IT
- IEC 615xx risk based Vs IEC 62443 risk based

Operational / Commercial Advantages

- Efficient management of plant / performance
- Remote supervision / travel
- Keep employees out of hazardous zone
- Diagnostics / MTTR
- IT technology lowering ICS costs
- Industry 4.0 / IOT / IIOT

Standards / Guidelines

IEC TC57 WG15

IEC 61784-4

Roadmap to Secure Control Systems in the Energy Sector

ISO 17799, ISO/IEC 2700x

NIST SP 800

BSI Grundschutz

NERC-CIP

IEC 62351

Common Criteria

NIST PSCRF

IEC 60870-5-10x

ISA 99

TÜV SÜD Certified Grid Control

IEC 61850

VDN TSM

WIB M-2784

GAO-04-140T

FIPS 140-2

CIGRE

VDEW

AGA 12

ISA-TR99

IEC / ISA-62443

DKE

INL

US-CERT Control Systems Security Center

Risk Reduction

IPSEC

Firewalls

IDS/IPS

CERT

RADIUS

Government legislation

International Standards

SIEM

802.1x

Solutions?

Antivirus

Active Directory

VPN

RSA

VLAN

AAA

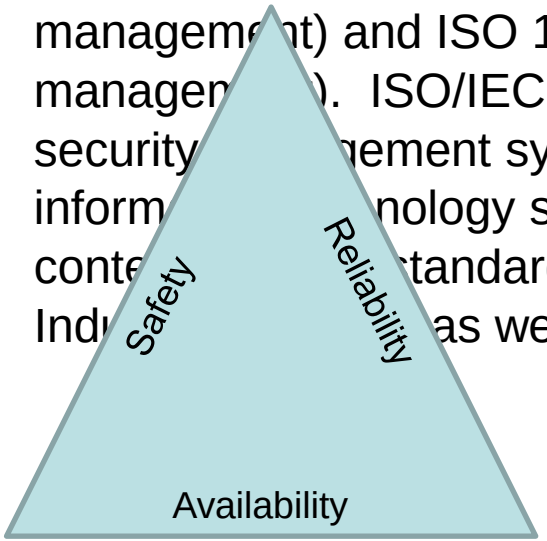
Gates / locks

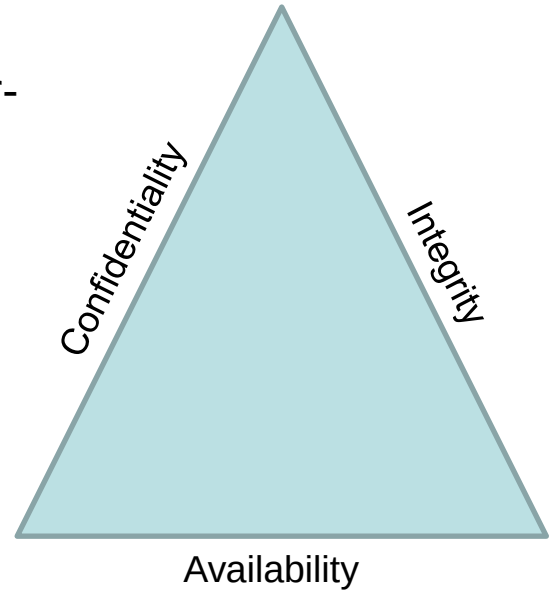
PKI infrastructure

Security guards

ISO 27000 Series

- The ISO 27000 series of standards have been specifically reserved by ISO for information security matters. This of course, aligns with a number of other topics, including ISO 9000 (quality management) and ISO 14000 (environmental management). ISO/IEC 27001 describes a cyber-security management system for business / information technology systems but much of the content of standards is applicable to Industrial as well.





IEC 62443

- All ‘Industrial Control Systems’
- Risk / lifecycle
- Security Level (SL)
- Access control
- Use control
- Data integrity
- Data confidentiality
- Restrict data flow
- Timely response to events
- Resource availability

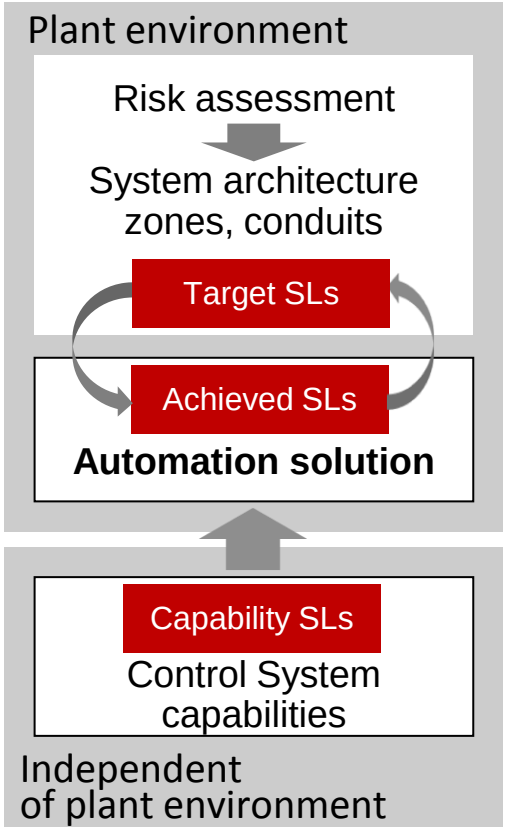
IEC 62443

SL 1 Protection against casual or coincidental violation

SL 2 Protection against intentional violation using simple means with low resources, generic skills and low motivation

SL 3 Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation

SL 4 Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation



IEC 62443

3-2 Security risk assessment and system design

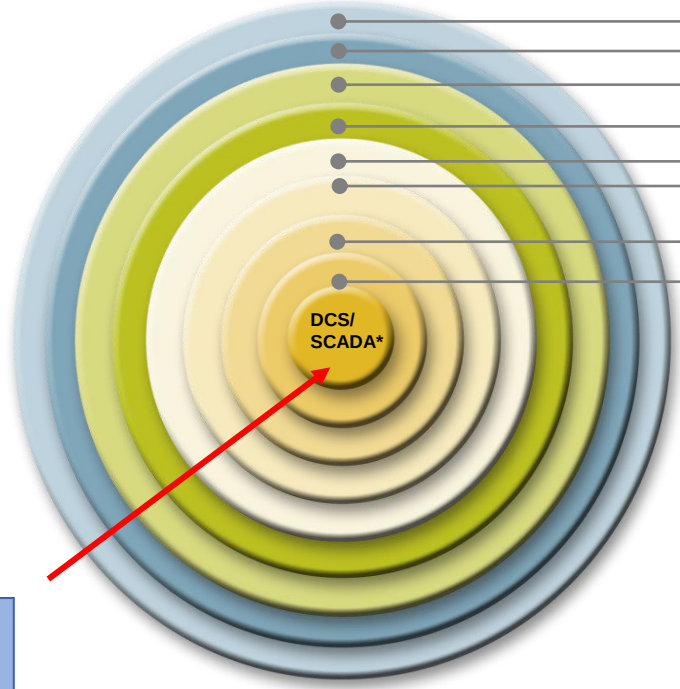
3-3 System security requirements and Security levels

1. **Part 3-2: asset owner / system integrator define zones and conduits with target SLs**
2. **Part 3-3: product supplier provides system features according to capability SLs**
3. **Capability SLs are deployed to match target SLs**

Issues for Security / IEC 62443

- How to ‘risk assess’?
- Detailed or high level?
- Where to get reliability data?
- Will insurance help?
- SIS & Connectivity
- SIS & Wireless
- SIS & Workstations
- CPNI ➔ ‘detect & respond’

Industrial IT Security



Potential Attack

***DCS:** Distributed Control System
SCADA: Supervisory Control and Data Acquisition

Plant Security

Physical Security
- Physical access to facilities and equipment

Policies & Procedures
- Security management processes
- Operational Guidelines
- Business Continuity Management & Disaster Recovery

Network Security

Security Zones & DMZ
- Secure architecture based on network segmentation

Firewalls and VPN
- Implementation of Firewalls as the only access point to a security cell

System Integrity

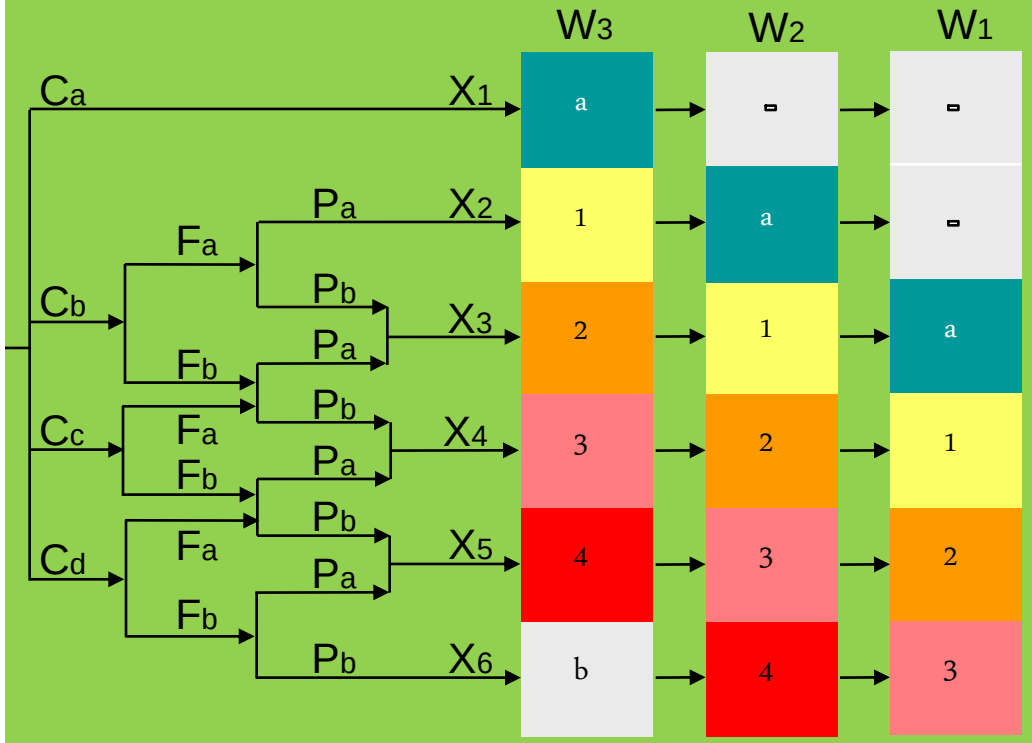
System Hardening
- Adapting system to be secure by default

User Account Management
- Access control based on user rights and privileges

Patch Management
- Regular implementation of patches and updates

Malware Detection and Prevention
- Anti Virus and Whitelisting

Risk Graph



Safety Integrity Levels SIL

a = no special safety requirements

b = individual safety system insufficient

Effect

- **Ca** Minor injury
- **Cb** Major, irreversible injury or death of one person
- **Cc** Death of several persons
- **Cd** Death of very many persons

Frequency and duration

- **Fa** Seldom to often
- **Fb** Frequent to constant

Danger prevention

- **Pa** Possible under cert. circum.
- **Pb** Nearly impossible

Probability of occurrence

- **W1** Very low
- **W2** Low
- **W3** Relatively high

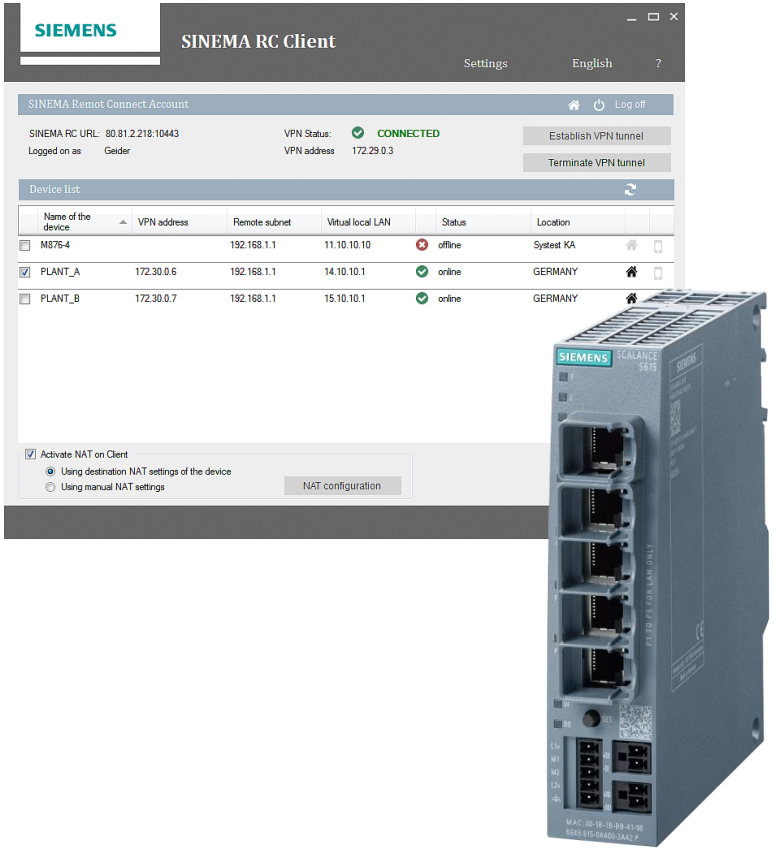
Risk Comparison

- Process Risk
- Machinery Risk
- Security Risk
- String of vulnerabilities
- Single vulnerability

PROFINET Security Concept

The PROFINET Security Concept
From the PROFINET Security Guideline

- Network Architecture – Security Zones
- Trust Concept – within Zones
- Perimeter Defence – Firewall/VPN
- Provision of Confidentiality and Integrity
- Transparent Integration of Firewalls



Possible Approach / Ideas

- No accepted risk assessment method
- Include ‘security’ team in safety hazard analysis
- Perform initial safety system security risk assessment
- Separate ICS security risk assessment
- SF/SIF security risk assessment

- ‘Layers of protection’ = ‘defence in depth’
- Add security management elements in FSM
- Follow existing 61508 Association guidance

- There is no silver bullet! We must add ‘layers’ now.

Any questions?

Peter Brown
Product Specialist
Siemens Customer Services
Mobile: 07808 825551
Email: brown.peter@siemens.com