Remote access in a secure manner ?

Sikkerhetssystemkonferansen 2006
Oslo 2-11-2006

Tor Olav Grøtan, NTNU / SINTEF Teknologi og samfunn

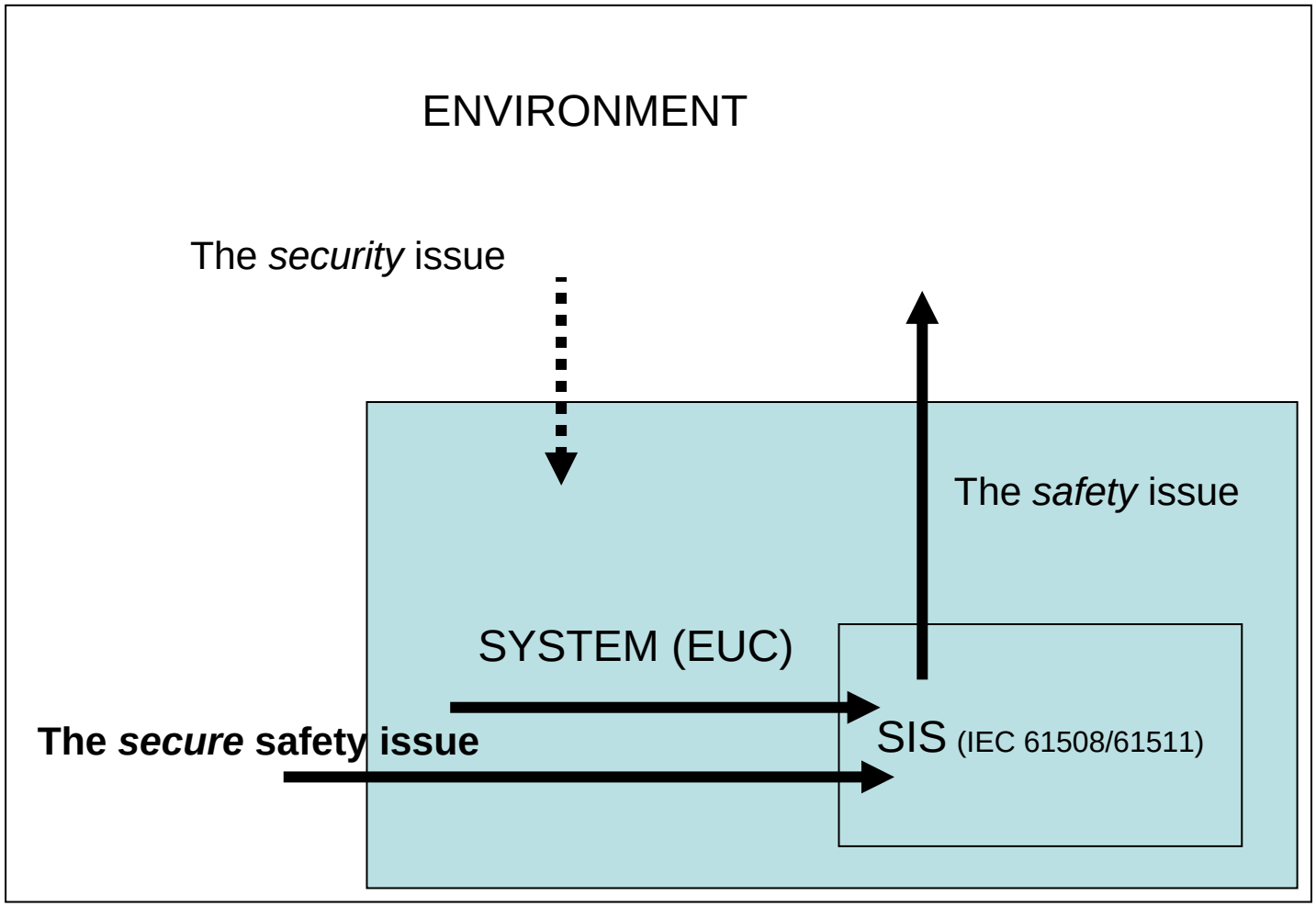
PDS forum: The SeSa project context

- Financed by Norwegian Research Council, owned by PDS Forum
- PDS forum
  - Norwegian acronym for ”Reliability of Computerised Control Systems”
  - Participants from oil companies, governmental bodies, vendors, consultants, engineering companies
- PDS objective/mission
  - Professional arena for exchange of experience between Norwegian vendors and users of Computerised Control Systems
    - Specifically on safety and reliability issues
- PDS method
  - IEC 61508/61511 based, with increased emphasis on systematic, common-cause failures
  - Main application: computerized safety systems in oil and gas offshore and onshore industry.
    - Safety Instrumented Systems (SIS)
    - E.g. Emergency Shut-Down (ESD) systems

The SecureSafety (SeSa) project

- Objective: Extension of PDS agenda, method and tools
  - Extend the PDS method to *cover failure modes that arise when a SIS on an oil platform is operated remotely* (via Internet connection)
- Scope:
  - Develop a framework for specifying *security* measures that are adequate for the purpose of *defending* the Safety Integrity Level (SIL) of the SIS, and provide practical guidance on its use
- Activities
  - Initial concept study on a case scenario (Floating Production Vessel)
  - Evaluation of theory, frameworks and standards
  - Identification of threats and (new) failure modes
  - Development of a SecureSafety specification method for the purpose of defending SIL levels
  - Development of practical guidance on use of the method

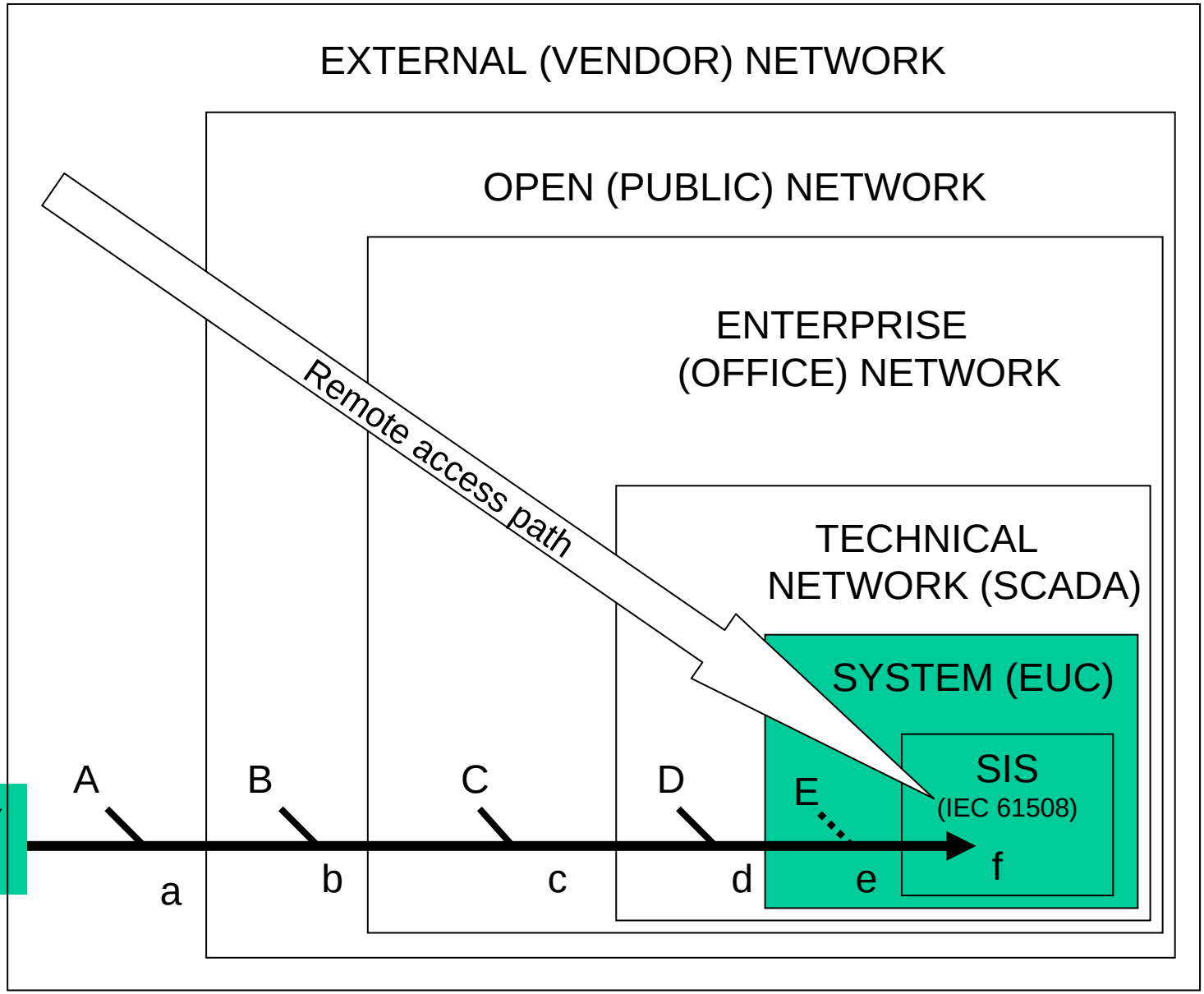
Conceptualization of SecureSafety



Structuring of SecureSafety : vs *SCADA security*, *Information security*

- Threats
  - A – E
- Security functions
  - a – f

The *SecureSafety* project issues

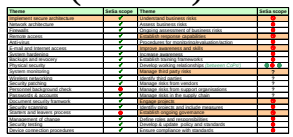


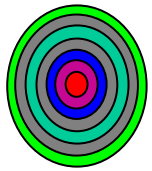
Outline of specification method

Establish overview of assumed threats and known weaknesses in remote access scenario

1. Detailing of requirements

(NISCC)



\+  +

”standard list” of threats/countermeasures

Pre-specification with assigned responsibilities (”protection profile” or ”security value chain”)

Responsible parties may be operator, contractor, …

2. Significant SIL impact ?

yes → Determine additional ”f+SIL” req. to handle residual threat → Qualifiable ? 3.

no

yes

Complete specification with assigned responsibilities

The underlying problems to be addressed

1. How to **organise and describe a proper defence** against (accumulated) threats along the remote access path
   - Understanding the interplay between
     - Threats A-E
     - Defences a-f
   - Standardisation ?
2. How to **model the impact on the SIL level** (potential SIL degradation)
   - Quantitative or qualitative ?
3. How to model, implement and measure the **combined ”f+SIL”**
   - Which has to be implemented alongside the (61508) safety function (in the same ”sandbox”)
     - ”f” = security function within SIS

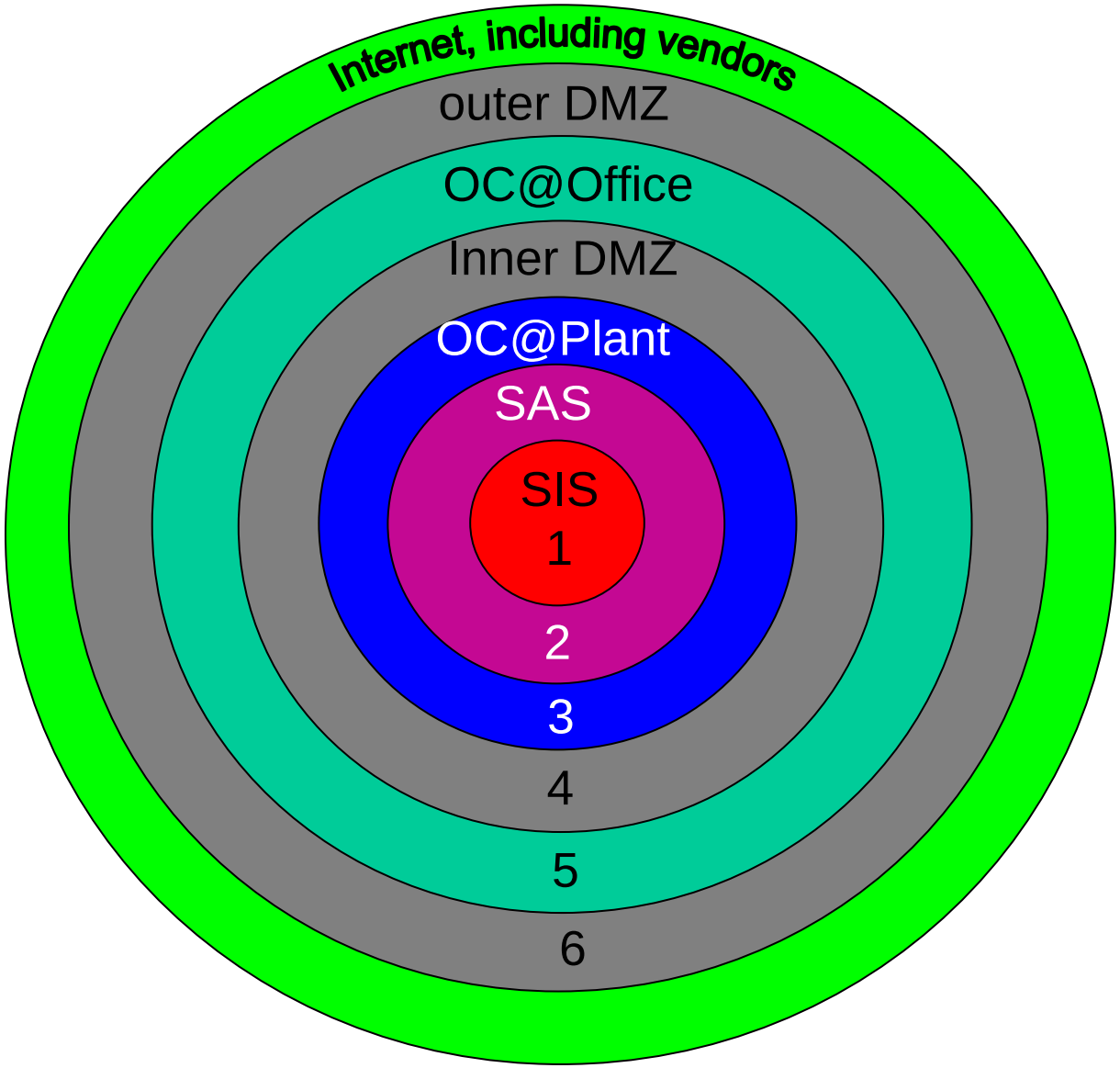
1: SeSa scope vs NISCC Good Practice Guide

Theme	SeSa scope	Theme	SeSa scope
Implement secure architecture	✓	Understand business risks	⊘
Network architecture	✓	Assess business risks	⊘
Firewalls	✓	Ongoing assessment of business risks	⊘
Remote access	✓	Establish response capabilities	⊘
Anti-virus	✓	Procedures for monitoring/evaluation/action	⊘
E-mail and Internet access	✓	Improve awareness and skills	⊘
System hardening	✓	Increase awareness	⊘
Backups and revocery	✓	Establish training frameworks	⊘
Physical security	✓	Develop working relationships *(between CoPs!)*	☺ ⊘ ☺
System monitoring	✓	Manage third party risks	?
Wireless networking	✓	Identify third parties	?
Security patching	✓	Manage risks from vendors	?
Personnel background check	⊘	Manage risks from support organisations	?
Passwords & accounts	✓	Manage risks in the supply chain	?
Document security framwork	✓	Engage projects	⊘
Security scanning	✓	Identifiy projects and include measures	⊘
Starters and leavers process	⊘	Establish ongoing governance	⊘
Management of change	✓	Define roles and responsibilities	⊘
Security testing	✓	Develop & update policy and standards	⊘
Device connection procedures	✓	Ensure compliance with standards	⊘

✓: within current scope **⊘ : not within (current) scope** **?: not decided**

Table based on "Good Practice Guide – Process Control and SCADA Security", NISCC, 2005

1. SeSa network architecture: Zone structure



- Zone structure seen from oil company (OC) point of view
- Vendors are ”external”
- Vendors are supposed to have a similar, but simpler structure
- The zone structure is used to set up a (dynamic) ”standard list” of threats and countermeasures to be considered at minimum
- The zone structure reflects the Norwegian oil/gas context, but is also similar to more generic ”secure SCADA” recommendations
  - E.g. NISCC
- SeSa : complementary to
  - SCADA security
  - O/G information security in general (e.g. OLF)

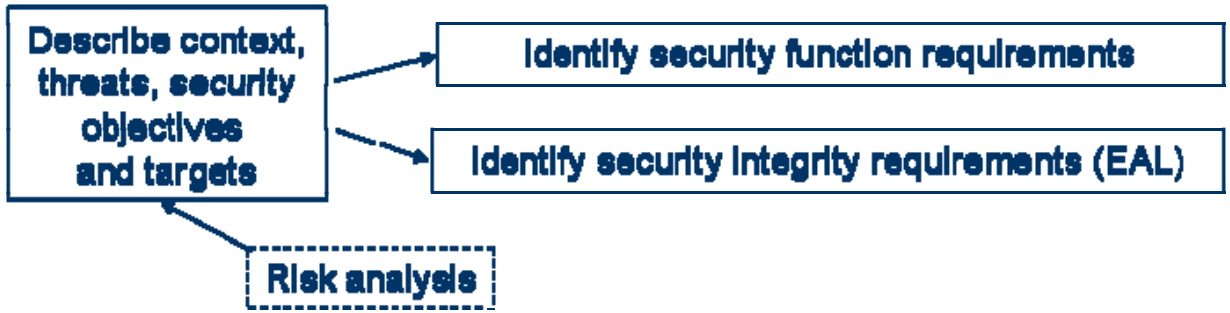
2. The security impact on SIL ?

- Meeting SIL requirements : based on three factors
  - The calculated Probability of Failure om demand (PFD)
  - Hardware redundancy due to IEC61508-2
  - Software requirements due to IEC61508-3
- It is reasonable to assume that a security threat may weaken only the assurances that are achieved by implementing the software requirements at a given SIL
  - A degradation table based on 61508-3 that reflects impacts from different (aggregate) security levels along the remote access path, could be construed *(however not within current SeSa scope)*
- Anyway, it would be (practically) wise to model the Probability of SIL Degradation (PSID) in two parts
  1. The likeliness that an adverse activity may reach the SIS border
     - Must be an ”epistemic” probability
  2. The level of resistance towards SIL degradation built into the SIS itself
  - Which would provide some engineering options!
    - Stop the threat before SIS
    - ”Tight system hardening” of SIS

3. A possible strategy for ”safe & secure” SIS

- IEC 61508 og ISO15408 ("Common Criteria for Security Evaluation")
- IEC 61508:

- ISO15408:



3. On IEC 61508 and ISO 15408

- Striking similarities
  - Assurances (SIL and EAL (Evaluation Assurance Level)) that signifies confidence in that the systems implement the proper functionality
  - Functionality derived from risk analysis
  - Both SIL and EAL assessments are based on good (and fairly similar) engineering principles for systems and software development
    - Although somewhat differently organised and expressed
- But also significant differences
  - ISO 15408: EAL assessment by third party
  - EAL could be reassessed for a given functionality
    - However within technological constraints (from COTS to ”handmade”)
  - ISO 15408 is less quantitatively oriented, and do not know ”fail-safe”
- EAL and SIL levels could support each other mutually
- Could we adopt the ISO 15408 Protection Profile approach?
- Warning: EAL levels are costly to establish and maintain

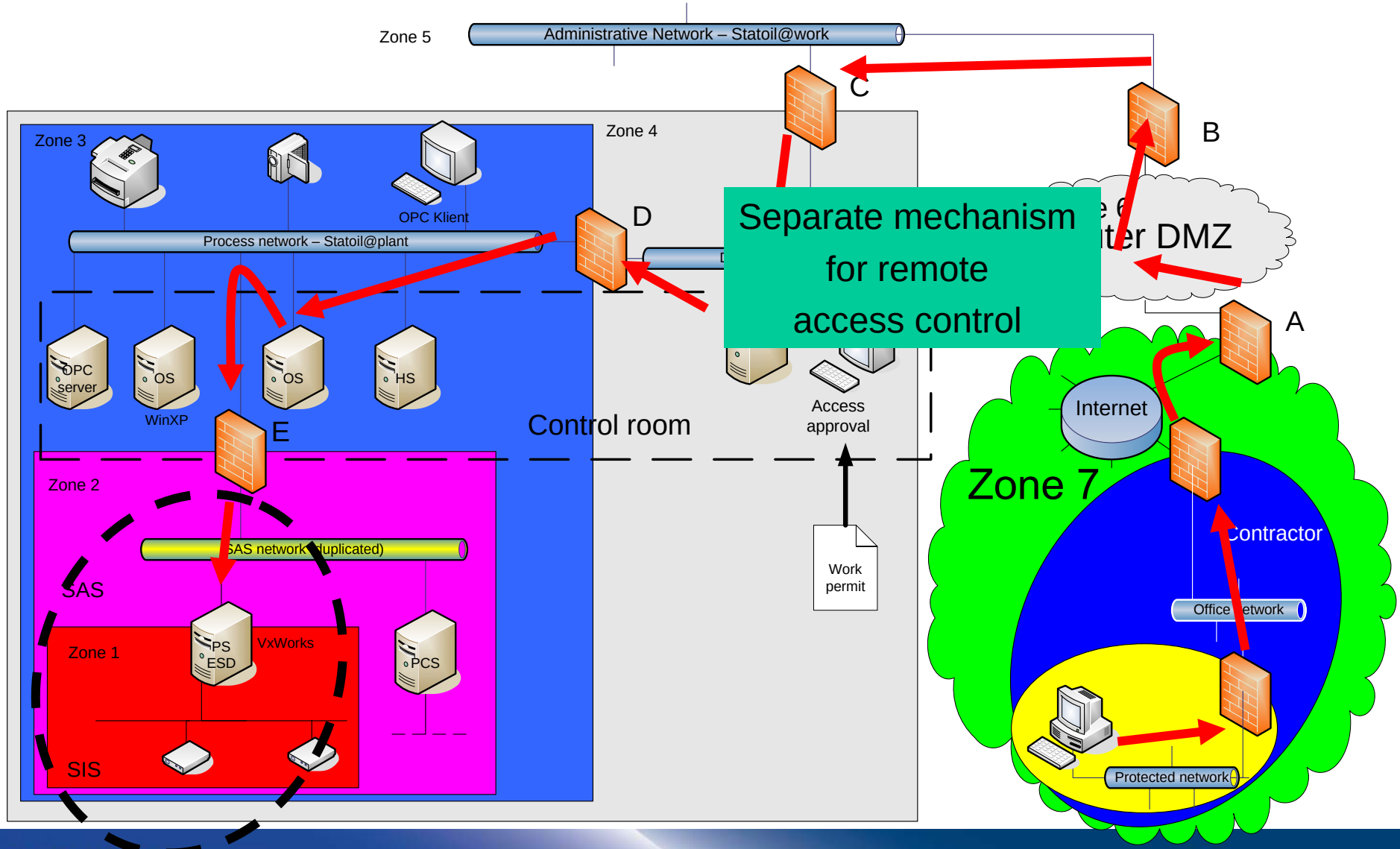
3. Combining SIL and EAL Kosmowski & al, ESREL 2006

nb! Security-functionality must be specified

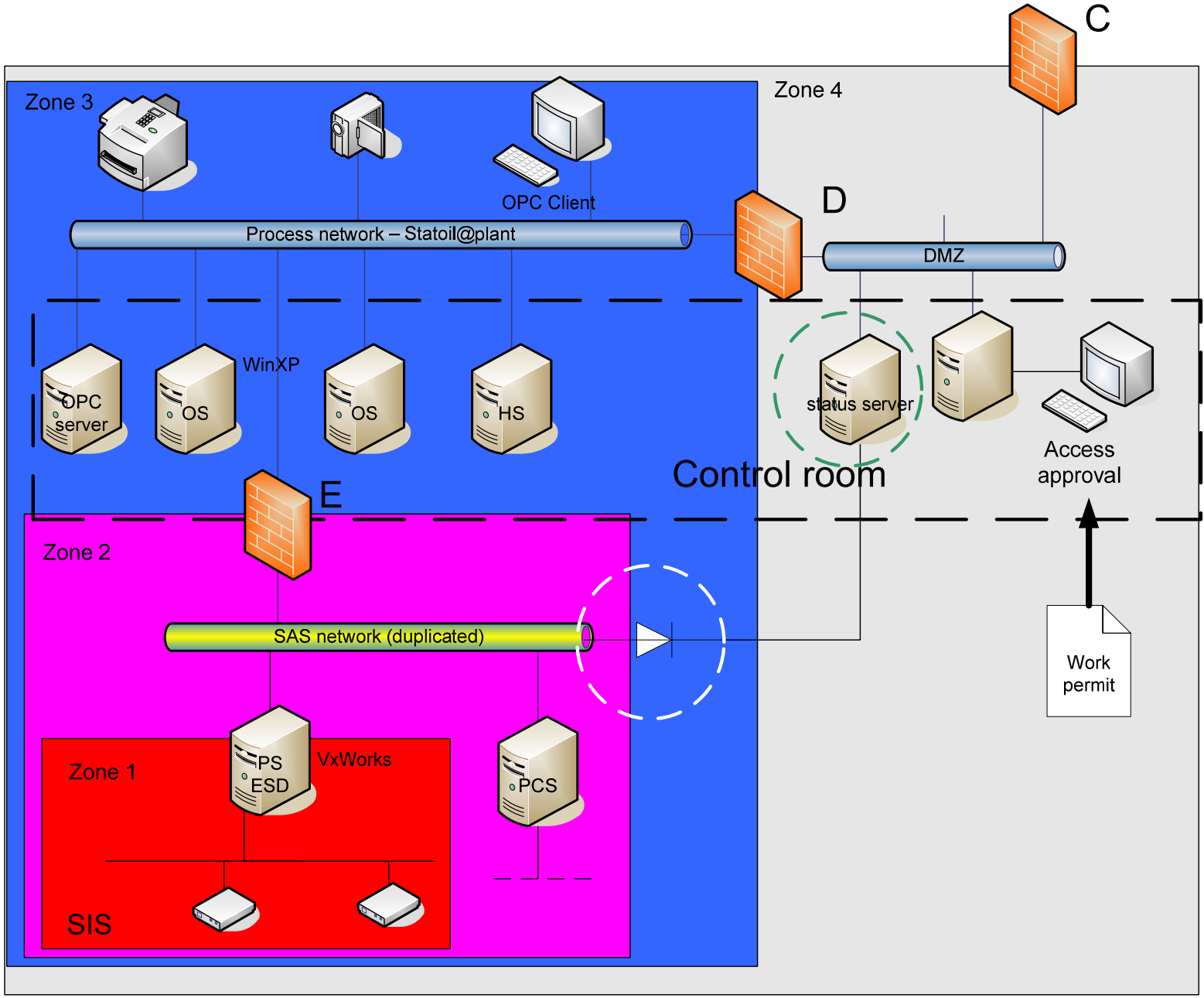
	EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
SIL 1							
SIL 2				X			
SIL 3							
SIL 4						X	

SeSa: Utilizing the parallells: SIL will ”carry” similar assurance

Guideline : applying the **method** on a ”typical” case, e.g



"Diode" for Read-Only



Residual (crucial) issues for SecureSafety

- ISO15408 and IEC 61508 : what can be achieved ?
  - EAL have a limited success compared to original scope
    - Due to cost and rigour
  - EAL levels may contribute to SIS resistance and/or shielding
    - Few examples of combined use
      - Poland (ESREL 2006)
      - Russia (CC 2006 conference)
- The ”insider threat” must not be allowed to take undue command
  - The IT security will carry a strong imperative on this!
  - ”Idiot-proofing” and ”deskilling” may be detrimental to safety culture
- The security challenge must be addressed jointly, but under leadership
  - Suitable metaphors: Security value chains, Protection Profiles (ISO 15408)
  - Recognised in NISCC ”Good Practice”
    - Third Party Risks
    - Ongoing Governance
- Sustained (secure) safety (”SIL i drift”)