SINTEF

SINTEF A1626 - Unrestricted

# Report

## The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems

Subtitle

**Author(s)**
Tor Olav Grøtan
Martin Gilje Jaatun
Knut Øien
Tor Onshus



**SINTEF Technology and Society**
Safety Research
Date

# SINTEF REPORT

**SINTEF Technology and Society**
Safety and Reliability

Address: NO-7465 Trondheim, NORWAY
Location: S P Andersens veg 5 NO-7031 Trondheim
Telephone: +47 73 59 27 56
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

TITLE

**The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems**

AUTHOR(S)

Tor Olav Grøtan, Martin Gilje Jaatun (SINTEF ICT), Knut Øien, Tor Onshus (NTNU)

CLIENT(S)

Multiclient – PDS forum

| REPORT NO. | CLASSIFICATION | CLIENTS REF. | |
|---|---|---|---|
| SINTEF A1626 | Unrestricted | Håkon Mathisen, Kongsberg Maritime | |
| CLASS. THIS PAGE | ISBN | PROJECT NO. | NO. OF PAGES/APPENDICES |
| | 978-82-14-04217-7 | 504052 | 43 |
| ELECTRONIC FILE CODE | | PROJECT MANAGER (NAME, SIGN.) | CHECKED BY (NAME, SIGN.) |
| SINTEF A1626 - SeSa report.doc | | Tor Olav Grøtan T.O. Grøtan | Stein Hauge Stein Hauge |
| FILE CODE | DATE | APPROVED BY (NAME, POSITION, SIGN.) | |
| | 2007-06-26 | Lars Bodsberg, Research Director Lars Bodsberg | |

ABSTRACT

Safety Instrumented Systems (SIS) are very important for the safety of Norwegian offshore installations. Partly as a consequence of evolving Integrated Operation concepts, a need for remote access to such systems from vendors external to the operating company, is expected. This kind of access will go through a number of networks used for other purposes, including the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SIS.

The SeSa (SecureSafety) project has developed a systematic and methodological approach to assess whether a given technological solution for remote access to SIS is acceptable. The approach is restricted to the security of the remote access path as such, but also takes into consideration the Safety Integrity Level (SIL) of the SIS itself. Assessment of proper SIL level to be defended through the method described herein is outside the scope.

The "SeSa method", comprises the following elements:

- A conceptual foundation for
  1) determining the SIL impact through the remote access path and
  2) combining security functionality with SIS implementation
- An architectural model and a checklist of threats and countermeasures along the remote access path
- A "Hazop -like" method for assessing the actual impact on SIL, based on use of the above mentioned checklist

The SeSa method has been developed in close cooperation with members of the PDS forum. The project has received financial support from the Norwegian Research Council

| KEYWORDS | ENGLISH | NORWEGIAN |
|---|---|---|
| GROUP 1 | Safety | Sikkerhet |
| GROUP 2 | Offshore | Offshore |
| SELECTED BY AUTHOR | Secure remote access | Sikker fjerntilgang |
| | Safety Instrumented System | Instrumentert sikkerhetssystem |

# TABLE OF CONTENTS

## *Preface*

The development of the SeSa method has been funded by participants in the PDS Forum and by the large-scale programme “Optimal Management of Petroleum Resources “ (PETROMAKS) of the Norwegian Research Council.

The PDS Forum was initiated in 1995 as a follow-up to the PDS research and development projects (see http://pds.sintef.no/). The main objective is to maintain a professional forum for development of safety systems within the petroleum industry and for exchange of experience between oil and gas companies, vendor companies, engineering companies, consultants, governmental bodies, and research organizations.

The following companies are participants of the PDS forum: ABB, Aker Kværner Engineering & Technology, BP Norge, ConocoPhillips Norge, Det Norske Veritas, Eni Norge, FMC Kongsberg Subsea, Honeywell, Invensys Systems Norge, Kongsberg Maritime, Nemko, Norsk Hydro, Norske Shell, Petrojarl Production, Saas systems, Safetec Nordic, Scandpower Risk Management, Siemens, Simrad Optronics, Statoil, Total E&P Norge, Directorate for Civil Protection and Emergency Planning (observer) and Petroleum Safety Authority Norway (observer).

The SeSa method complements the PDS handbooks for quantifying the safety unavailability and production loss of Safety Instrumented System (SIS):

- Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2006 Edition, SINTEF Report STF50 A06030, ISBN 82-14-03898-7, April 2006. (Distributed by Sydvest, www.sydvest.com)
- Reliability Data for Safety Instrumented Systems, – PDS Data Handbook, 2006 Edition, SINTEF Report STF50 A06030, ISBN 82-14-03898-7, April 2006. (Distributed by Sydvest, www.sydvest.com)

The PDS handbooks may be used to calculate Safety Integrity Levels (SIL) in line with the IEC 61508 standard.

The PDS handbooks are continuously updated through PDS Forum.

# 1 SUMMARY

Safety Instrumented Systems (SIS) according to the IEC 61508/61511 [22], [23] series of standards and the PDS[1] method [21], is very important for the safety of Norwegian offshore installations. Partly as a consequence of evolving *Integrated Operation* concepts, a need for remote access to such systems from vendors external to the operating company, for the purpose of operation and maintenance, is expected. This kind of access will go through a number of networks used for other purposes, including the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SIS.

This report describes a systematic approach to assess whether a given[2] technological solution for remote access to SIS implies an unacceptable risk, in terms of jeopardizing the *safety integrity level* (SIL) of the SIS. As the notion of *acceptability* of such remote access to SIS may encompass many aspects beyond the scope of this report, we emphasise that acceptability is defined as follows in this report: *the access is acceptable if no significant impact on the SIL level is revealed by use of the SeSa method, provided that the SIS requirements and SIL level in question are assessed properly in advance, according to the proper rules and standards.*

The approach assumes that the offshore site installation, the operating oil company as well as the external vendor complies with the Information Security Baseline Requirements (ISBR) for oil & gas operations [12]. Hence, the scope of this approach and report is restricted to the security of the *remote access path to the SIS* (including the SIS itself) as such. Furthermore, the assessment is limited to the design and requirement level, and do not take into account issues related to implementation, operation and maintenance of the actual technical solutions.

The methodological approach described herein, the "SeSa method", comprise the following elements

- A conceptual foundation for
  1. determining the SIL impact through the remote access path and
  2. combining security functionality with SIS implementation (technically speaking, obtaining *implicit* security assurances through safety integrity levels, SIL)
- A checklist of threats and countermeasures along the remote access path, based on a prescribed multi-layered architecture ("onion model").
- A "Hazop[3]-like" approach for assessing the actual impact on SIL, based on use of the above mentioned checklist

The conceptual foundation for the method is discussed in chapter 3. In chapter 4, the method is outlined in a procedural view. In chapter 5, a "checklist" for specification of threats and countermeasures as well as its sources and architectural presumptions (the "onion model") is presented.

[1] The PDS method has been revised and is compatible with the IEC 61508, however with a stronger emphasis on systematic, common-cause failures. The PDS method has been applied in numerous projects and in many different contexts. The main application, however, has been to computer-based safety systems in the offshore and onshore oil and gas industry

[2] That is, a solution within a range of possible solutions delineated by a prescribed structure which is part of the method

[3] the "Hazard and operability analysis" (HAZOP) is a structured approach to verifying threats/hazards and their countermeasures

In addition, an example of a technical solution assessed through the SeSa method, is given in chapter 6.

# 2 Introduction

## 2.1 Background

Safety Instrumented Systems (SIS) according to the IEC 61508/61511 series of standards and the PDS method [21], are very important for the safety of Norwegian offshore installations. E.g., an Emergency Shutdown System (ESD) constructed according to these principles is often the ultimate guarantor for fail-safe properties at such installations. Neither IEC61508 nor the PDS method is currently oriented towards security issues.

In relation to the emergence of Integrated Operations (IO) [30], it is foreseen that the demand for remote operation and maintenance of such systems using Internet connections will be inevitable. The general picture therefore seems to be that remote access to the safety and control systems have been and will be implemented gradually over the forthcoming years. The actual need for such an open access and the total risk associated with it has however not been within the scope of this project.

One of the main questions related to remote access will however be whether this kind of connection is *technically secure*, that is, whether operators and authorities can be confident that such a connection is not tampered with, misused, or in any other way channelling or enforcing an unwanted[4] *impact on the SIS* itself that can raise significant doubt on its claimed Safety Integrity Level (SIL). Answering this question is the mission of the SeSa method. The output of the method is considered to be relevant if the SIL level to be defended, have been assessed in advance according to relevant standards and guidelines.

A main objective of this report is therefore to extend the PDS method to cover (new) failure modes that arise when a SIS on an offshore installation is operated and maintained remotely, via an Internet connection. However, while the PDS method targets the SIS and not its surroundings, the main bulk of security protection will presumably reside in the access path, not within the SIS itself. I.e., preferably, the security measures outside the SIS should suffice. If not, the final line of security defence will have to be implemented *within* the SIS. In the former case, we can treat the security and safety issues separately. In the latter case however, we must also address the combined safety and security within the SIS. Although the former case is the most attractive from a security protection viewpoint, the SeSa method also accommodates the latter, more complicated case.

Hence, the primary focus of this report is the technical issues that are necessary to specify a recommended *remote access path* to SIS, in order to assess whether it is secure. However, a number of underlying issues will also be addressed:

1. The conceptual foundation for assessing whether a residual security threat at the SIS border represent an unacceptable threat to the SIL (implying a degradation of the SIL)

[4] The distinction between security and safety is among other things (see also [4]), a distinction between *intentional* (malicious/hostile) and *accidental* acts or circumstances. This distinction may be somewhat blurred in cases where e.g an employee *unintentionally* and *indirectly* introduces a (hostile) agent, e.g by connecting a virus-infected laptop to a SAS network segment. For our purpose, protection against such threats is mainly an ISBR issue, cfr chapter 2.3.

2. In cases where a residual risk has to be handled by a security function within the SIS, will the "assurances" implicitly provided by the SIL itself, also suffice as assurances in relation to this security function?

Industrial safety and (computer) security issues are two related but still rather different, fields of theory and practice that we seek to combine in the SeSa method. This will not be unproblematic, and some problems are already manifested in the mixed vocabulary that we have to employ when we are addressing safety and security, respectively. Practitioners within both fields are concerned about this challenge. As further discussed in [4], combining these two approaches into a coherent whole is not achieved solely through a technical report, but our modest hope is that this report may contribute to such a development.

### 2.2 Scope

The scope of this report is to describe a framework for specifying *security* measures and demonstrate their adequacy for the purpose of *defending* the Safety Integrity Level (SIL) of the SIS when it is accessed remotely, and provide practical guidance on the use of the framework.

This implies that both confidentiality of information and issues relating to regularity are specifically defined as outside the scope. I.e., for the purposes of this report we are less concerned with the possibility that the SIS shuts down a platform too soon or too often, as long as it does shut down when necessary. Note however that the (counter)measures recommended in this report *may* have a beneficial impact also on issues that are out of scope, e.g regularity.

### 2.3 Presumptions and limitations

Note that the *SecureSafety (SeSa) method*:

1. is only applicable to the specific scope – it is not a generic method that can applied directly for other purposes
2. is based on a "pre-structuring" of the remote access path, thus it is not directly applicable for solutions that do not comply with this structure.

Furthermore, the use of r*emote access path specifications* produced by this method is only valid on the following presumptions:

1. that the operating company, as well as the vendor, complies with the Information Security Baseline Requirements (ISBR) for oil & gas operations [12], so that "ordinary" security threats (e.g. introduction of virus due to illegitimate use unsecured of laptops) can be ruled out from the SeSa threat picture
2. that the operating company also pursues a more general focus on SAS[5] security, ensuring that the SIS is properly isolated from and thus *independent*[6] of other SAS subsystems, so that access to e.g. PCS cannot be used as a platform for unauthorized access to SIS
3. that the operating company must actively audit and control the implementation of the remote access path specified herein, all the way from the external vendor to the SIS. As the successful operation of this path comprises a number of actors, we will use the metaphor "security value-chain" to signify this aspect.

[5] In the available literature, e.g. [2], the term "SAS" is denoted "SCADA" (Supervisory Control and Data Acquisition) systems

[6] According to Petroleum Safety Authority (Ptil) Regulations

Finally, we emphasize that due to the dynamic nature of the field of IT security, in which threats and vulnerabilities emerge and are revealed rather abruptly, it is not possible to develop security specifications that can warrant against future threats. Thus, the recommendations herein are only applicable given that they are carefully scrutinized by experts in the field of application (this scrutinizing is an integrated part of the SeSa method), and caution is taken continuously with regard to their practical use.

## 2.4 Standards and guidelines

Both traditional safety standards and information security standards are relevant to this report, and in addition, there are several guidelines or "good practice" guides on SCADA security that have an impact on the discussion.

### 2.4.1 The safety standards

IEC 61508/61511 constitute the safety reference point and "hub" for all discussions in this report, as they define the SIL to be protected against degradation by means of the SeSa method.

The current issues of IEC 61508/61511 keep security issues explicitly out of their scope. However, Schoitsch [7] argues that it is possible and feasible to combine safety and security focus within the conceptual framework of IEC61508/61511, and explicitly points at the similarities between these standards and ISO 15408. Also Kosmowski et al. [8] argue that these standards can be combined, and explicitly presents a mapping table between the confidence level scales (EAL and SIL) associated with the use of ISO 15408 and IEC61508/61511, respectively.

### 2.4.2 The "pure" security standards of relevance for this work

The following security standards are of relevance or special interest for our scope:

- ISO 15408 Information technology - Security techniques - Evaluation criteria for IT security [24]
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, 2005 [25]. Previous versions known as BS 7799 and ISO/IEC 17799.

### 2.4.3 SAS (SCADA) security

The following standards/guidelines address the security of industrial SCADA systems in general.

- NISCC Good Practice Guide – Process Control and SCADA Security, PA Consulting Group, October 2005 [2]
- Good Practice Guide – Firewall Deployment for SCADA and Process Control Networks. NISCC, UK. 2005 [3]
- Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST special publication 800-82 (initial public draft), September 2006 [4]

### 2.4.4 Other initiatives of relevance

OLF has issued a guideline specifying Information Security Baseline Requirements (ISBR) for oil & gas operations [12]. These requirements are based among others on ISO/IEC 27001 [25] and

input from industry representatives, and can be considered as a set of minimum requirements for information systems used in the petroleum industry.

### 2.5 Abbreviations and terms

| | |
|---|---|
| CC: | Common Criteria [24] |
| COTS: | Commercial Off-The-Shelf |
| DMZ: | De-Militarized Zone |
| DoS: | Denial of Service |
| EAL: | Evaluation Assurance Level [24]. A scale for confidence levels that can be obtained by the use of ISO15408 |
| ESD: | Emergency Shutdown System |
| EUC: | Equipment Under Control |
| FPSO: | Floating Production, Storage and Offloading |
| FW: | FireWall, see Appendix B |
| GW: | GateWay |
| IFEA: | Industriens Forening for Elektroteknikk og Automatisering (The Association for Electrotechnics and Automation in Industry) |
| IO: | Integrated Operation |
| IP: | Internet Protocol |
| IPsec: | IP Security Protocol |
| ISBR: | Information Security Baseline Requirements |
| ISMS: | Information Security Management System |
| MAC: | Medium Access Control [address] |
| NFA: | Norsk Forening for Automatisering |
| NCS: | Norwegian Continental Shelf |
| OLE: | Object Linking and Embedding |
| OLF: | Oljeindustriens LandsForening (National Oil Industry Association) |
| OPC: | OLE for Process Control |
| PCS: | Process Control System |
| PDS: | Reliability of computer based safety system (Pålitelighet av Databaserte Sikkerhetssystemer) |
| PSD: | Process Shutdown System |
| RAT: | Remote Access Tool |
| Proxy: | An entity acting on behalf of another activity, thereby offering security for the latter. See appendix B for explanation of *firewall proxy* |
| Safety: | Protection against unintended, accidental acts or circumstances that may impact SIS |
| SAS: | Safety and Automation System |
| SCADA: | Supervisory Control and Data Acquisition. |
| Security: | Protection against intended, malicious or hostile acts or circumstances that may impact SIS |
| SIL: | Safety Integrity Level |
| SIS: | Safety Instrumented System |
| SJA: | Safe Job Analysis |
| SSL: | Secure Sockets Layer |
| SOIL: | Secure Oil Information Link |
| TCP: | Transmission Control Protocol |
| UDP: | User Datagram Protocol |
| UTP: | Unshielded Twisted Pair |
| VPN: | Virtual Private Network |
| OS: | Operator Station (part of SIS) |
| PS: | Process Station (part of SIS) |

HS: History Server (part of SIS)
SS: Status Server (part of SIS)

### 2.6 Why information security is important in Integrated Operations

As commercial off-the-shelf (COTS) computer equipment is coming into use in control system environments, these environments may potentially be exposed to the same threats as home PC users. Thus, when control systems are reachable from Internet connections, these issues must be handled seriously. Also other threats than those arising from "hackers" should be considered, see section 5.1.2

Sandia National Laboratories has assembled a list of vulnerabilities commonly found in critical infrastructure control systems [31]. These vulnerabilities are organized in categories: Those related to PCS administration, those related to PCS networks, and those related to PCS platforms.

Some examples of relevant incidents from other sectors are briefly presented below, solely for the purpose of indicating the potential damage and risk. Other incidents are known, but cannot be reported publicly.

**Worcester Air Traffic Communications**
*In March 1997, a teenager in Worcester, Massachusetts disabled part of the public switching network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport.*

*Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress.*
*The attack also knocked out phone service to 600 homes in the nearby town of Rutland.*

**Maroochy Shire Sewage Spill**
*In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.*

**Northeast Power Blackout**
*In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. Additionally, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345kV transmission lines in Northern Ohio trip due to contact with trees. This eventually initiates cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. 61,800 MW load is lost as 508 generating units at 265 power plants trip.*

**Bellingham, Washington Gasoline Pipeline Failure**
*In June 1999, 237,000 gallons of gasoline leaked from a 16" pipeline and ignited 1.5 hours later causing 3 deaths, 8 injuries, and extensive property damage. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. "Immediately prior to*

*and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation." A key recommendation from the NTSB report issued October 2002 was to utilize an off-line development system for implementing and testing changes to the SCADA database.*

**Incidents on the Norwegian Continental Shelf**
*In August 2005, a virus infected an oil company corporate network [26] and spread to machines that were not centrally managed. 185 machines were infected. It seems that only luck and swift reaction from the system administrators prevented a major production shutdown.*

# 3 Modelling security impact on Safety Integrity Level (SIL)

Security and safety are related concepts. As discussed in [4], "secure safety" can be generally interpreted as the protection of the Equipment Under Control (EUC) vs. its environment, for the purpose of maintaining confidence in the protection of the environment vs. the EUC. In our case, the *secure safety* concept is more narrowly interpreted; securing the remote access path to SIS, to ensure that the SIL of the actual SIS is not compromised by deliberate[7] misuse of the remote access path.

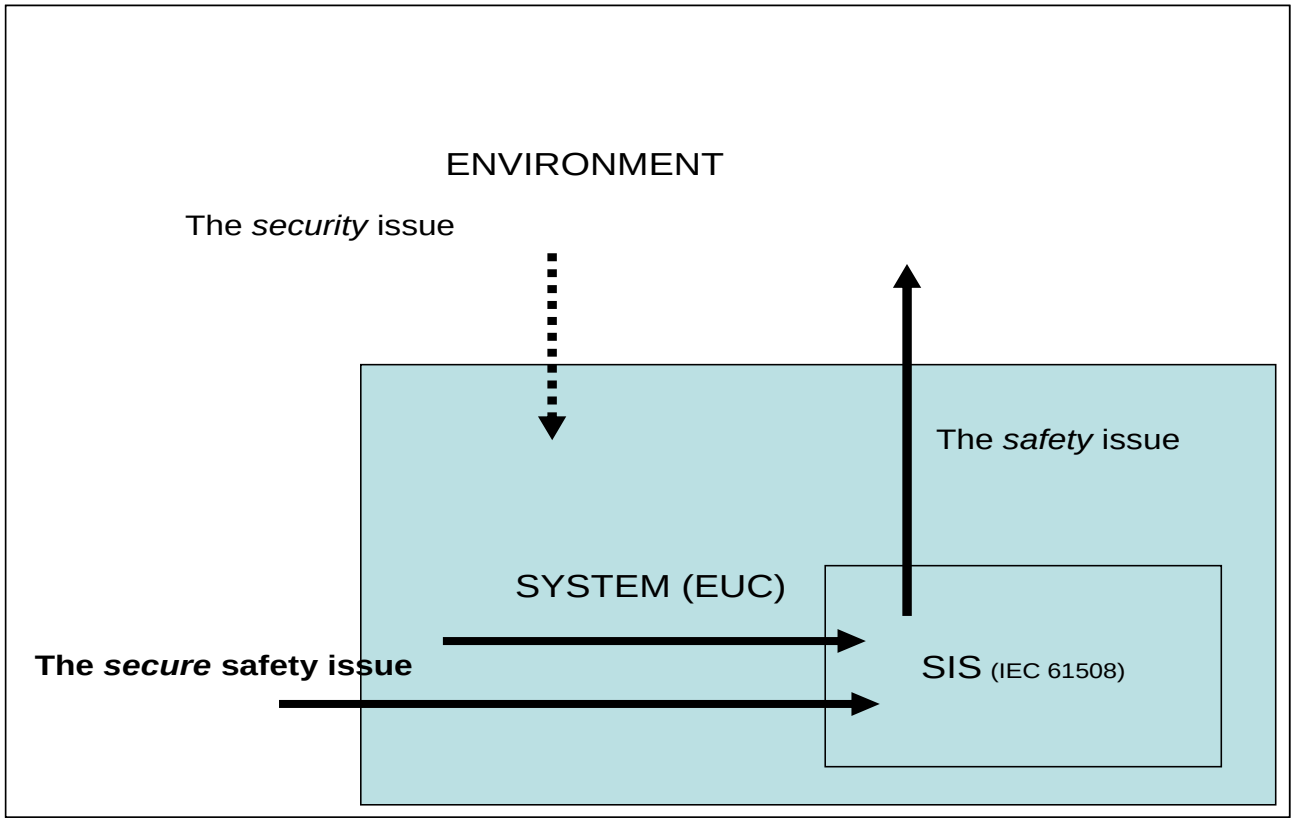


**Figure 1: The Secure Safety issue**

Figure 1 above illustrates this concept, in which the SIS is responsible for a crucial safety function (e.g an emergency shutdown system (ESD), a process shutdown system (PSD), or a fire&gas detection system).

[7] As stated in chapter 2.1, the introduction is of a security threat is not necessarily the direct act of a hostile "hacker", but can also occur as the result of lack of mindfulness, e.g. using laptop without updated virus protection.

The actual SIS complies with given SIL (Safety Integrity Level) requirement. The SIL requirement is usually the result of some kind of risk analysis. The mission of the SIS concerns the safety of the plant, and the SIL level is established according to IEC 61508 on the premises that the SIS is an autonomous, isolated system. The remote access path challenges these premises, and it is our challenge to assess whether it actually also jeopardizes the SIL of the SIS.

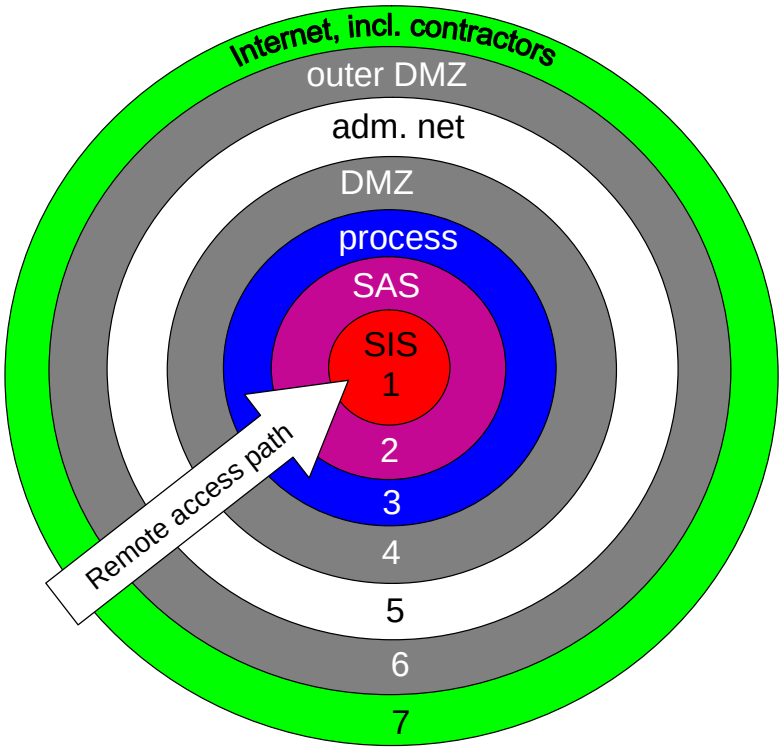


**Figure 2: Remote Access Path**

In Figure 2, the general notion of "environment" is replaced by a layered network architecture, incorporating the overall technical data network (SAS) on the plant, the oil company office network enveloping the technical network, the open, public network (e.g. the Internet) which makes it possible to make a connection between the company owning the EUC, and the network of the external vendor that is allowed to operate and maintain the SIS. It should be noted that this architecture, incorporating the enveloping of the technical network by the office network, is due to good-practice recommendations, e.g. in [2]. Thus, the challenge is to provide a set of security functions in order to counter for a set of feasible threats along the remote access path penetrating this architecture. The security functions will serve a number of objectives, which in the IT security arena commonly are termed confidentiality, integrity, availability, accountability, non-repudiation etc (as defined by ISO 15408).

As we will see below, a crucial question will be whether the security functions external to SIS offers sufficient protection, or if not; a security function *within* the SIS itself (e.g. a password authentication and authorisation scheme) is also needed.

### 3.1 Organising and describing the remote access path

In order to assess the effect of the security functions along the remote access path, threats and functions are organised according to a prescribed layered architecture (Figure 2). A checklist (in chapter 4) attached to this architecture is provided to facilitate this analysis. The checklist is partly based on recognised standards and recommendations, and thus benefit from the implicit confidence carried by these. However, due to the dynamic nature of IT security threats, experts familiar with the oil/gas domain must for each case explicitly consider whether the threat/function picture is sufficient.

### 3.2 Assessing the impact on SIL

The assessment of whether the SIS meets the SIL requirement is based on the four factors:

- the calculated Probability of Failure on Demand (PFD)
- architectural hardware requirements as given in to IEC 61508-2
- management of functional safety
- software requirements as given in IEC 61508-3, that is, requirements that are either "recommended", "highly recommended" or "not recommended"

It is reasonable to assume that the security impact will affect mainly the software requirements. That is, any security threat may maximally weaken the assurances that are achieved by implementing the software requirements for a given SIL. This premise could, at least in theory be represented by a degradation table that reflects different (aggregate) security levels along the remote access path. We could then, in principle, quantify the degradation of SIS. The higher the SIL, the higher the sensitivity in relation to security threats. Such an approach would then also require a classification scheme for the residual threat vs. SIS.

This approach is however considered unpractical, because

1. there is no empirical experience available to classify the threats in our context
2. it will be a challenging task to agree on a (theoretical) degradation mapping
3. the risk of adverse activity at the SIS border cannot be modelled by (random) frequency but will depend on the motivation and capability, as well as the dedication and persistence, behind the assumed threat
4. it would not be meaningful to compensate[8] for a potential degradation with a "higher" SIL.

Rather, we propose that the assessment must be performed as an expert judgement, based on the well-known "HAZOP" (Hazard and Operability Analysis) technique and principles, answering **one main question**: does the proposed remote access path pose a substantial impact on a given SIL, or not.

### 3.3 Combined safety and security functions in SIS

If the expert judgement concludes that there is no significant likelihood that an adverse activity would reach the SIS border, then the case is closed and the specification is complete. On the other side, if this conclusion cannot be reached in the first round, and it is also not possible to introduce new access path security functions external to SIS to accomplish this in a second round, then

[8] That is, if a plant requires a SIL3 ESD in the outset, and then is perceived to be at risk as a result of the remote access path,, thus the requirement is "raised" to SIL4 in order to serve as a "confidence buffer"

another set of questions must be raised: Is it possible to specify an additional[9] security function within the SIS (e.g. authentication and access control), will this function suffice, or will it by itself interfere with and compromise the SIL implementation in the SIS?

The answer to the latter questions is not only a matter of functional characteristics, it is also a matter of *confidence* in the function being properly implemented. As discussed in [4] and [6], the structural similarities between IEC61508 and ISO15408 are at first glance appropriate for our purpose. However, ISO 15408 is a very rigid standard, and it cannot be expected that products certified according to ISO 15408 will be available for SIL applications.

Nevertheless, as pointed out by Kosmowski et al. [8] , it is possible to map the so called *assurance levels* ("EAL") defined in ISO 15408 with the SIL levels of IEC 61508/61511. This is indicated in Figure 3 below. From the two mapping points identified, a linear mapping could be extrapolated. This mapping should however be interpreted very cautiously; it only signifies that the *assurance (confidence) level* for a given security function at (e.g.) EAL 6, corresponds to the *degree of confidence* that is related to a SIL 4 function.

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

**Figure 3: Mapping of assurance level inherent in SIL to Common Criteria (ISO 15408)**

We can utilise this in the following way: if the required security function within the SIS has been qualified to a given SIL level, it will implicitly carry a level of confidence corresponding to the (extrapolated) mapping in Figure 3. As the sensitivity to security-induced disturbances is proportional to the SIL level, we can conclude that the *SIL itself will carry adequate security assurance, if the security function is explicitly defined as part of the SIS functional specification*[10]. It will also be reasonable to assume that safety and security will not interfere with each other. However, as this conclusion is rather general, this must also be judged and verified through the HAZOP process.

[9] As will be clear from the next chapter, some baseline (security) requirements to SIS, e.g. systerm hardening, will be mandatory. This type of requirement will however overlap with requirements derived from the SIL

[10] This point deserves some clarification. We have earlier stated that IEC 61508/61511 does *not* address security. A "security function explicitly defined as part of SIS functional specification" will thus not originate from IEC 61508/61511. However, it might still be part of the SIS specification of the vendor. Our point is that if this is so, and if the SeSa checklist requirements of chapter 5 are met, *then* the SIL verification will implicitly carry the necessary confidence.

The practical result from a verification of this conclusion may e.g. be that a password protection mechanism built into a SIS system that also is “hardened” according to the SeSa checklist, implicitly is verified through the SIL requirement.

# 4 Overview of the SeSa method

Prescribed/recommended steps in using the SeSa model on a given case are illustrated in Figure 4.

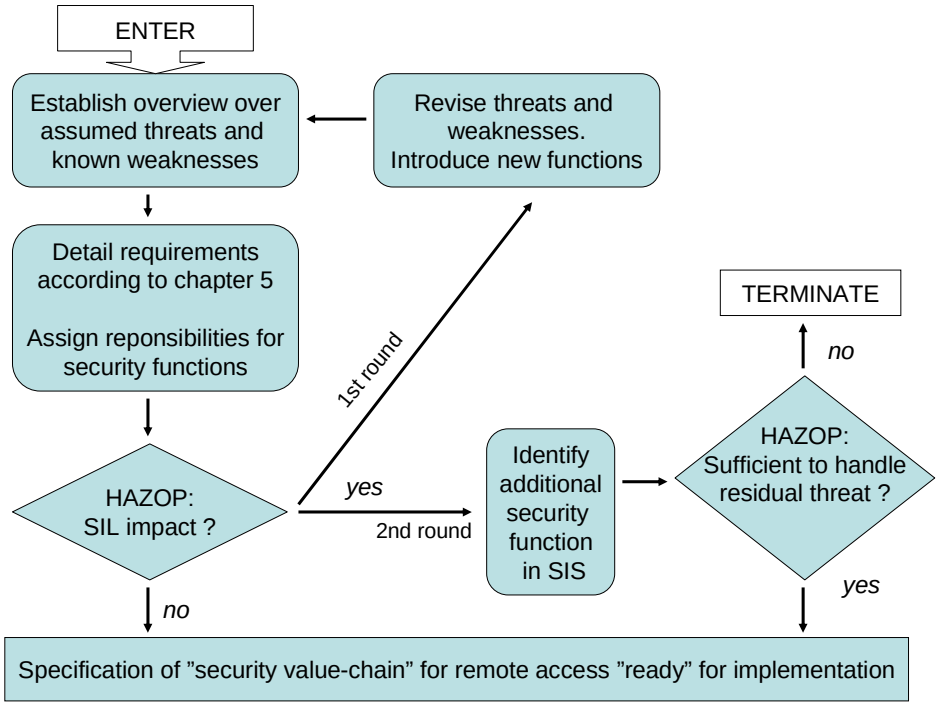


**Figure 4: The SeSa method**

In short, the method comprises the following steps:

1. Establish overview of threats and known weaknesses, and existing security mechanisms in SIS
2. Develop requirements specification of the "security value chain" for the remote access path, using the specification framework in chapter 5
3. Determine the impact on SIS/SIL through a HAZOP-oriented analysis
4. If impact cannot be ruled out, try another round based on updated threat/weakness picture and additional requirements (1st round)
5. If impact still cannot be ruled out, identify additional security functions within SIS, and assess through HAZOP whether this (will) provide sufficient protection vs. the residual threat (2nd round).
6. If confidence in security functions within the SIS perimeter is needed according to the previous step, assess whether the assurance level implicitly carried by the specified SIL level, is sufficient
7. If "success" is not achieved after the 2nd round, the proposed solution should be discarded.

However note that:

I. The HAZOP (Hazard and Operability Analysis) technique is well-established in industrial safety. In the SeSa method, we use the HAZOP principles in much the same way as the CORAS project (see [32]); that is, use HAZOP to identify threats and verify whether these threats are mitigated by the proposed design of the remote access path.

II. The SeSa use of HAZOP means that if no "problem" remains after all *explicitly known* possibilities have been examined exhaustively, the "conclusion" must be that the proposed solution is *per definition* "secure". However, as we stated in chapter 2, there will always be a possibility that something is overlooked, or that new threats and vulnerabilities emerge or is revealed at a later time. *The SeSa method cannot account for this type of (epistemic) uncertainty.* Such potential "flaws" in the judgement must be handled in retrospect, when they are revealed.

III. More generally, a "successful" use of the method gives a result that is "ready" for implementation only due to the SeSa scope and its limitations, as stated in chapter 2!

Note that there is a possibility to "bypass" the method above, for the purpose of read-only access. If a "diode" solution according to chapter 5.4.3 is implemented, the above method is no longer relevant, as the threat towards SIS is eliminated from the outset. However, any read-only solution *not* complying with chapter 5.4.3 must be evaluated by means of the SeSa method.

Also note that a read-only solution may be a valuable contribution to security, even though a separate full-fledged access solution must be implemented to service a smaller number of external users. In broad terms it is reasonable to argue that the fewer users that are allowed to access SIS, the narrower the access path may be constructed, thus lessening strain on the security solution and the possibility of impact on SIS.

# 5 The SeSa framework for requirements specification

The analytical framework comprises three different perspectives:

a) NISCC good practice guide [2]
b) BSI threat tables [13]
c) I3P preliminary report [10]

The resulting framework is exemplified as a layered architectural model, also known as "the onion model" (section 5.2), and a checklist for threats and countermeasures within this architecture (Table 3).

## 5.1 Background

There are quite a lot standards and guidelines available on this issue. The SeSa framework comprises the following.

### 5.1.1 NISCC SCADA Good Practice Guide

The good practice guide from NISCC [2] provides some input on applicable threats to our test case. Under the heading "Assess business risk", there is a section with an example list of high-level threats: "[...] denial of service, targeted attacks, accidental incidents, unauthorised control, or [malware] infections."

In addition to threats from one zone to another, we have indirect threats from within – such as configuration errors in firewalls and other security mechanisms – that in turn leave the system vulnerable to outside attackers. This includes issues such as weak passwords or insufficient authentication mechanisms.

If integrated operations (IO) evolve to the extent that contractors need to access their respective equipment over an open internet, the industry as a whole will be rendered vulnerable to Denial of Service (DoS) attacks, as there currently is no certain method to protect against a targeted DoS-attack. Possible countermeasures include alternative access networks, in addition to having a well-functioning system for handling information security incidents.

| Theme | SeSa scope | Theme | SeSa scope |
|---|---|---|---|
| **Implement security architecture** | **Yes** | **Understand business risks** | **Yes** |
| Network architecture | Yes | Assess business risks | Yes |
| Firewalls | Yes | Ongoing assessment of business risks | No |
| Remote access | Yes | **Establish response capabilities** | **No** |
| Anti-virus | Yes | Procedures for monitoring/evaluation/action | No |
| Email and Internet access | Yes | **Improve awareness and skills** | **Yes** |
| System hardening | Yes | Increase awareness | Yes |
| Backups and recovery | Yes | Establish training networks | No |
| Physical security | Yes | Develop working relationships | Yes |
| System monitoring | Yes | **Manage third party risks** | **No** |
| Wireless networking | Yes | Identify third parties | No |
| Security patching | Yes | Manage risks from vendors | No |
| Personnel background check | No | Manage risks from support organisations | No |
| Passwords and accounts | Yes | Manage risks in the supply chain | No |
| Document security framework | Yes | **Engage projects** | **Yes** |
| Security scanning | Yes | Identify projects and include measures | Yes |
| Starters and leavers process | No | **Establish ongoing governance** | **Yes** |
| Management of change | Yes | Define roles and responsibilities | Yes |
| Security testing | Yes | Develop and update policy and standards | Yes |
| Device connection procedures | Yes | Ensure compliance with standards | No |

**Figure 5: NISCC good practice and SeSa scope**

The complete NISCC good practice guide exceeds the scope of this report, and only the items checked in Figure 5 are actually incorporated in our case. In the following we present a partly annotated list of relevant points in connection with the checked items.

### 5.1.2 BSI Baseline Protection Manual (BPM)

To ensure broader coverage, the threat catalogue regarding deliberate acts from the BSI Baseline Protection Manual [13] has been compared with the case at hand, and examples of relevant threats have been highlighted (identified as T 5.X in Table 3 – note that the threats are primarily used as input to the model; no attempt has been made to provide an exhaustive mapping). Note that only threats relevant to the "secure safety" issue are considered; threats regarding e.g. confidentiality may be relevant in a broader business case, but will not be covered here.

The BSI BPM contains a wide variety of threats with varying degrees of detail. Thus there are some threats that are very general, while other threats are specific to e.g. Novell Netware (which may be a bit outdated) and other named operating systems. Some threats appear to be specialisations of more general threats described earlier; these we have omitted. Also note that the currently available version of the BPM is from 2004, which means that newer threats are not covered. Threats relating to "deliberate acts" from the BPM that are relevant to the Secure Safety issue are listed in Table 1.

| BSI BPM threat number | Description |
|---|---|
| T 5.1 | Manipulation or destruction of IT equipment or accessories |
| T 5.2 | Manipulation of data or software |
| T 5.6 | Attack |
| T 5.8 | Manipulation of lines |
| T 5.9 | Unauthorised use of IT systems |
| T 5.10 | Abuse of remote maintenance ports |
| T 5.15 | "Inquisitive" staff members |
| T 5.16 | Threat posed by internal staff during maintenance/administration work |
| T 5.17 | Threat posed by external staff during maintenance work |
| T 5.18 | Systematic trying-out of passwords |
| T 5.19 | Abuse of user rights |
| T 5.20 | Abuse of administrator rights |
| T 5.21 | Trojan horses |
| T 5.23 | Computer viruses |
| T 5.24 | Replay of messages |
| T 5.25 | Masquerading |
| T 5.27 | Repudiation of a message |
| T 5.28 | Denial of services |
| T 5.37 | Determining access codes |
| T 5.38 | Misuse of remote inquiry |
| T 5.39 | Infiltrating computer systems via communication cards |
| T 5.42 | Social engineering |
| T 5.48 | IP spoofing[11] |
| T 5.50 | Abuse of the ICMP protocol |

[11] Spoofing: To forge the originator ("from") address in an IP packet. Frequently used to make attack traffic look as though it is originating from a trusted system

| BSI BPM threat number | Description |
|---|---|
| T 5.51 | Abuse of routing protocols |
| T 5.53 | Deliberate misuse of protective cabinets for reasons of convenience |
| T 5.54 | Deliberately causing an Abnormal End |
| T 5.55 | Login bypass |
| T 5.56 | Temporary free-access accounts |
| T 5.60 | By-passing system guidelines |
| T 5.61 | Misuse of remote access to management functions on routers |
| T 5.62 | Misuse of resources via remote IT systems |
| T 5.66 | Unauthorised connection of IT systems to a network |
| T 5.67 | Unauthorised execution of network management functions |
| T 5.68 | Unauthorised access to active network components |
| T 5.70 | Manipulation by family members or visitors |
| T 5.72 | Misuse of e-mail services |
| T 5.73 | Impersonation of a sender |
| T 5.78 | DNS spoofing |
| T 5.79 | Unauthorised acquisition of administrator rights [under Windows NT] |
| T 5.81 | Unauthorised use of a cryptomodule |
| T 5.82 | Manipulation of a cryptomodule |
| T 5.83 | Compromising cryptographic keys |
| T 5.84 | Forged certificates |
| T 5.85 | Loss of integrity of information that should be protected |
| T 5.86 | Manipulation of management parameters |
| T 5.87 | Web spoofing |
| T 5.88 | Misuse of active contents |
| T 5.89 | Hijacking of network connections |
| T 5.91 | Disabling of RAS access security mechanisms |
| T 5.92 | Use of the RAS client as RAS server |
| T 5.93 | Permitting use of RAS components by third parties |
| T 5.109 | Exploitation of system-specific vulnerabilities [with Apache web server] |
| T 5.110 | Web bugs |
| T 5.112 | Tampering with ARP tables |
| T 5.113 | MAC spoofing |
| T 5.115 | Overcoming the boundaries between VLANs |

**Table 1: Applicable threats from BSI Baseline Protection Manual**

### 5.1.3 I3P

In a white paper from the Institute for Information Infrastructure Protection (I3P [10]), six vulnerability categories are presented, as reproduced in Table 2.

| Vulnerability category | Description and Examples |
|---|---|
| System Data | • Lack of understanding of what data is considered sensitive, how it should be separated and protected |
| Security Administration | • Lacking policies, standard procedures, training and corporate/industry security plans<br>• Formal configuration management needed for upgrades, legacy plans and patching |
| Architecture and Design | • No integrated security in SCADA designs. Security must be an add-on<br>• Centralized storage or control mechanisms are single points of failure |
| Platforms | • Patching, backups, passwords, OS security, application security and security policies for access control and file sharing are needed<br>• Physical access control is lacking |
| Networks and communication | • Wireless security, monitoring, encryption, access control, boundary security and standards for implementation are all needed |
| Incident Response and Handling | • Response plans are lacking, as well as backup and disaster recovery plans<br>• Forensic data collection and analysis is needed<br>• Redundant operational capability is beneficial |

**Table 2: Characterized Vulnerabilities from I3P [10]**

These vulnerability categories highlight the need for an ISMS in relation to SCADA installations. The categories most directly applicable to this report are Architecture and Design (No integrated security in SCADA designs) and Networks and communication (encryption and access control).

### 5.2 The "onion model" and the resulting checklist

Figure 6 depicts a layered access model from an operator's point of view (note similarity with the layered model presented in [27]). This model is based on two demilitarized zones (DMZ); one serving as a buffer between the operator's network and "the outside world", while other separates the operator's administrative network (which may span several installations) from the process network (which typically is restricted to a single installation).

All contractors must be considered "external" just like the rest of the Internet, since the operator has no physical control over the contractor's networks (operators may impose contractual restrictions with respect to how and with what equipment contractors are allowed to access the operators' networks, but will have limited means of verifying these arrangements on a continuous basis).

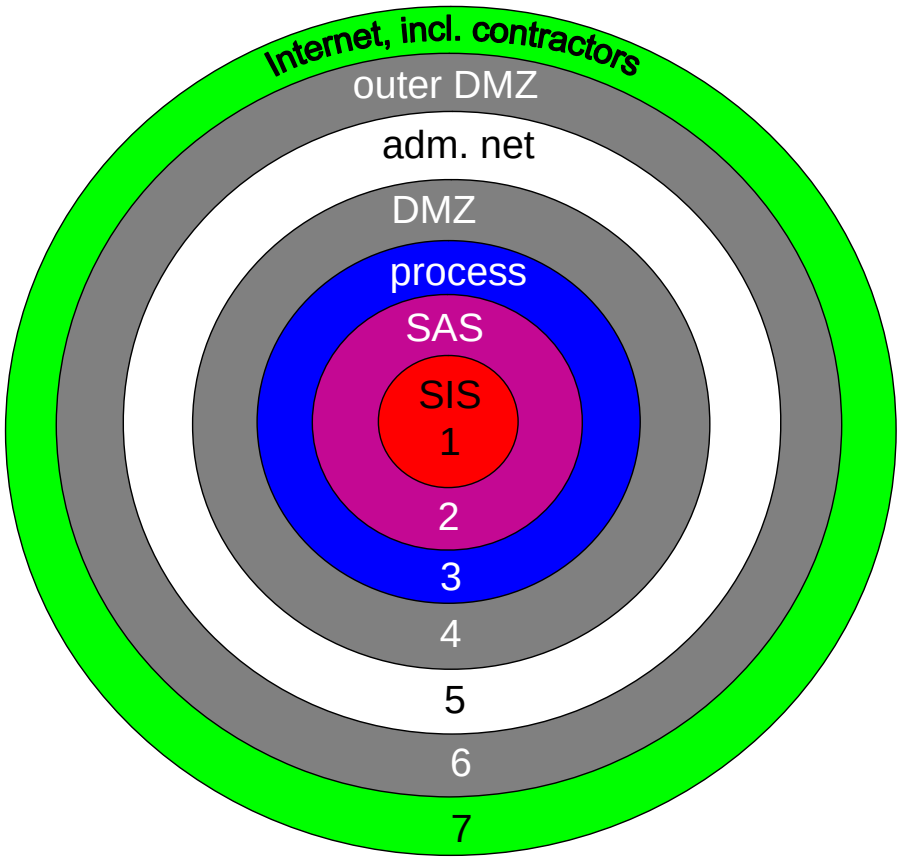


**Figure 6: Layered model for remote access**

The layered model of Figure 6 can be argued on several levels. First, the separation of layers 1-3 from the surrounding is based on the requirement for SIS autonomy, as stated in [1]. Furthermore, the separation of the process network from the administrative network is as recommended in the NISCC good practice guide [2]. Finally, the outer DMZ protects against all external actors, with special mechanism to allow authorized contractors to access the appropriate parts of the operator's network.

As the operator has no physical control over the contractors' networks, the latter are likely to differ from installation to installation. By contractual obligations, operators should mandate a minimum layering as illustrated in Figure 7, where equipment used to access the operator's network is placed in a zone separated from the general office network (in the following, zone 1 in the contractor's network is referred to as zone c1, etc. Zone 3 in the contractor's network is equivalent to zone 7). Note that since access in this model conceptually always originates from the contractor, there is no need for the contractor to have a DMZ between its network and the internet – a single barrier (i.e. firewall) is sufficient. This is also illustrated in Figure 9.

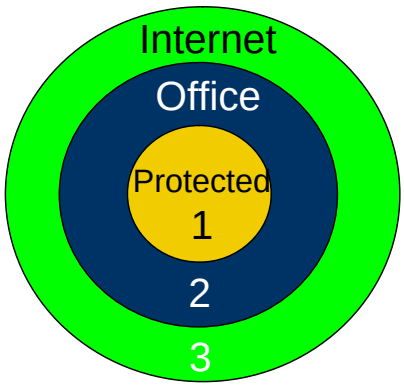


**Figure 7: Layered network model on contractor side**

### 5.2.1 "Standard list" of threats and countermeasures in the onion model

The threats that have been identified thus far are listed in Table 3. The threats are as a rule described as originating from an adjoining zone, but the ultimate goal for a given attack may be to traverse all interfaces to affect the innermost zone, e.g. in order to illegitimately shut down an oil installation. Note that no pre-compiled list of threats can ever be considered "complete" for any real networked system; the threats presented here must be treated as a starting point that as a minimum must be compared with the network to be studied. Threats that are found to be not applicable or irrelevant must be documented as such, and a site-specific analysis must be performed to uncover additional threats.

A conservative threat analysis must adhere to Kerckhoffs' principle [11], and assume that an attacker has access to all pertinent information regarding a system (network topology, configuration) except passwords, encryption keys, etc.

The threats in Table 3 are further elaborated in chapter 6. All threats in the table are annotated with "ultimate impact"; this is to be understood as the lowest zone where the specific attack has an effect. For instance, if an attacker can manipulate (e.g. change or inject bits) traffic from contractor to SIS as it passes through the internet, the attack originates in zone 7, and affects data in zone 7, but since the data is carried in to SIS, the ultimate impact is in zone 1. If the ultimate impact is different from zone 1, this implies that (at least) one additional attack is required in order to affect zone 1.

Additional strength can be gained by requiring the use of "certified" machines from zone 4 and inwards, but this is strictly speaking outside SeSa scope.

As stated in section 2.3, we assume that the ISBR[12] are adhered to when considering threats; e.g since configuration control is already a requirement it should not have to be stated here. However, in some cases where it is particularly important, e.g. to avoid that "alien" equipment is connected to technical networks, this is also stated explicitly.

| From Zone | To zone | Threat | Ultimate impact on zone | Countermeasure | Notes |
|---|---|---|---|---|---|
| 7 | c1 | Attack on c1 | 1 | Configuration control, administrative measures<br>(Specifically: Not allowed to access c1 from c2)<br>Firewalls and c1 tightly configured, hardened | T 5.21, T 5.23 T 5.88 T 5.110 |
| 7 | 7 | Malware planted in contractor's "secure zone" | 1 | Configuration control, administrative measures | T 5.21, T 5.23 T 5.88 T 5.110 |
| | | Manipulation of legitimate traffic | 1 | Encrypt and authenticate | T 5.2, T 5.8, T 5.24, T 5.25 |
| 7 | 6 | Attack on firewall A | 6 | Firewalls must be tightly configured and patched | T 5.6 |
| | | Attack on other resource in zone 6 | | Don't have other resources in DMZ<br>Other resources that *have* to be in the DMZ must be tightly configured (hardened) | If FW A is correctly configured, it shouldn't be possible to attack other resources in DMZ. |
| 7 | 6 | Attack on DMZ gateway | 5 | Tight configuration and hardening.<br>Strong authentication<br>Restrict access to DMZ GW to pre-defined addresses | T 5.62<br>If firewall A lets all hosts connect to DMZ GW, and firewall B allows all traffic from DMZ GW |
| 6 | 6 | Attack on DMZ GW from other resource in DMZ | 5 | Tight configuration and hardening. | |
| 6 | 5 | Attack on Firewall B | 5 | Firewalls must be tightly configured and patched | |
| | | Spoof traffic to bypass FW B | | Detect spoofed traffic<br>Encrypt and authenticate | T 5.48, T 5.89 |
| 5 | 5 | Manipulation of legitimate traffic | 1 | Encrypt and authenticate<br>Network segmentation | T 5.2, T 5.8, T 5.24, T 5.25<br>Overall / concrete impact must be handled in advance by SJA (with respect to regularity etc.) |
| | | Malware planted in operator's administrative net | | Configuration control, administrative measures, malware detection,<br>IDS (?) | T 5.21 T 5.23 |

| From Zone | To zone | Threat | Ultimate impact on zone | Countermeasure | Notes |
|---|---|---|---|---|---|
| 5 | 4 | Attack on Firewall C | 4 | Firewalls must be tightly configured and patched<br>Each firewall must be a separate physical unit.<br><br>"Internal administrative access" must be treated on the same premises as C1 access (same access path, same hardening requirements) | Additional resilience may be gained by requiring each firewall to originate from a different manufacturer |
| | | Attack on other resource in zone 4 | | Don't have other resources in DMZ<br>Other resources that *have* to be in the DMZ must be tightly configured (hardened) | |
| 5 | 4 | Attack on DMZ gateway | 3 | Tight configuration and hardening<br>Explicit filtering rules on FW D to restrict access to host that has legitimate need for access. | If firewall C lets all hosts connect to DMZ GW, and firewall D allows all traffic from DMZ GW . |
| 4 | 4 | Attack on DMZ GW from other resource in DMZ | 3 | Don't have other resources in DMZ<br>If read-only status server is placed here: tight configuration & hardening | |
| | | Attack on Firewall D | | Firewalls must be tightly configured and patched.<br>Each firewall must be a separate physical unit. | Additional resilience may be gained by requiring each firewall to originate from a different manufacturer |
| 4 | 3 | Spoof traffic to bypass FW D | 3 | Detect spoofed traffic<br>Encrypt and authenticate | T 5.25 |
| 3 | 3 | Attack on Firewall E | 2 | Firewalls must be tightly configured and patched.<br>Each firewall must be a separate physical unit. | Additional resilience may be gained by requiring each firewall to originate from a different manufacturer |
| 3 (C1) | 3 | Equipment used for | 1 | Reduced service. Tightest possible hardening | T 5.19 |

| From Zone | To zone | Threat | Ultimate impact on zone | Countermeasure | Notes |
|---|---|---|---|---|---|
| | | unauthorized purposes | | | Additional risk reduction may be achieved through use of inner DMZ proxy (Least privilege) |
| 3 (Internal) | 3 | Equipment used for unauthorized purposes | 1 | Reduced service<br>Alternative “citrix” service | T 5.19<br>Partly outside SeSa scope – here restricted to the impact offshore users may have on the remote access path. |
| 3 | 2 | Unauthorized equipment | 2 | Work permits, configuration control.<br>Specific mechanisms (e.g. MAC-filtering) may enforce rejection of unauthorized equipment<br>Must not be able to “stimulate” resident malware from C1 (firewalls can prevent communication from C1 to any equipment not specifically authorized) | T 5.66<br>ISBR-enforced |
| 2 | 2 | Users with legitimate access to a given sub-system gain access to other subsystems | 2 | Firewall E to separate zone 3 and 2, and also separate between different subsystems | T 5.55 |

**Table 3: (Checklist:) Threat and Countermeasure summary**

### 5.3 Access modes

If a substantial part of the need for remote access is “read-only”, it is strongly recommended to consider such an approach. A solution on such a basis will in itself be easier to verify (cf. chapter 4, Figure 4) than a “full” solution. If read-only and read-write solutions need to coexist, a “double” solution will imply that the entry to the latter solution may be even more restrictive, and thus increasing the chance for success in the “1st round” in Figure 4. On the other hand, a read-only solution may potentially be reachable from a wider (looser) set of operational contexts, on the vendor side.

Hence, for a further reduction of complexity in solutions, we propose that remote access is divided into three coarse categories:
0 – no access
I – read-only access
II – full read/write access to SIS (OS)

These can be further refined as follows:
I-1 – snapshots of SIS state (via “information diode” – see 5.4.3). In principle, this is the equivalent of a CCTV transmission of the terminal display.
I-2 – real time readout of SIS with possibility of specifying parameters.
II-1 – real time data transmission between installations, e.g. from a PS on one platform to a PS on another. This implies machine-machine communication without user intervention.
II-2 – interactive read/write access to SIS (OS)

When dividing computer networks in different zones, firewalls are most commonly used. For a brief introduction on firewalls and how they function, see Appendix B: What is a firewall?”

#### 5.3.1 Access examples

The various access options described in section 5.1 can now be mapped to the layered models as illustrated in Figure 8, where it is assumed that “information diode” functionality (see 5.4.3 for details) is available.

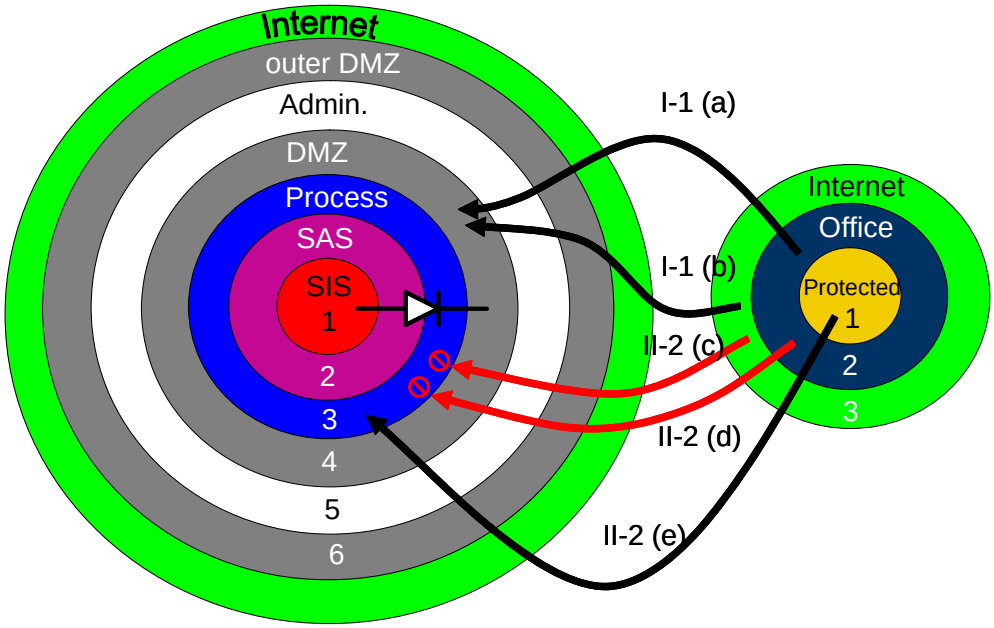


**Figure 8: Allowed and rejected access attempts**

a) Allowed access from contractor's office network to DMZ (e.g. to read historical data from SIS)
b) Allowed access from internet to DMZ
c) Rejected (blocked) access from contractor's office network to process network
d) Rejected (blocked) access from internet to process network
e) Allowed access from contractor's protected network to process network (via broker function in DMZ)

Note that e.g. prevention of access from contractor's office network cannot be done reliably by packet filtering alone. Also note that the outer DMZ will have additional access control mechanisms that are not explicitly described here.

### 5.4 Physical mapping

An example of how the layered "onion" models presented above may be translated into a physical network configuration is presented in Figure 9. Note that while the doctrine of "defense in depth" mandates that each of the firewalls A-D should be implemented as separate units, a functionally equivalent configuration using only two units with three interfaces each is possible.

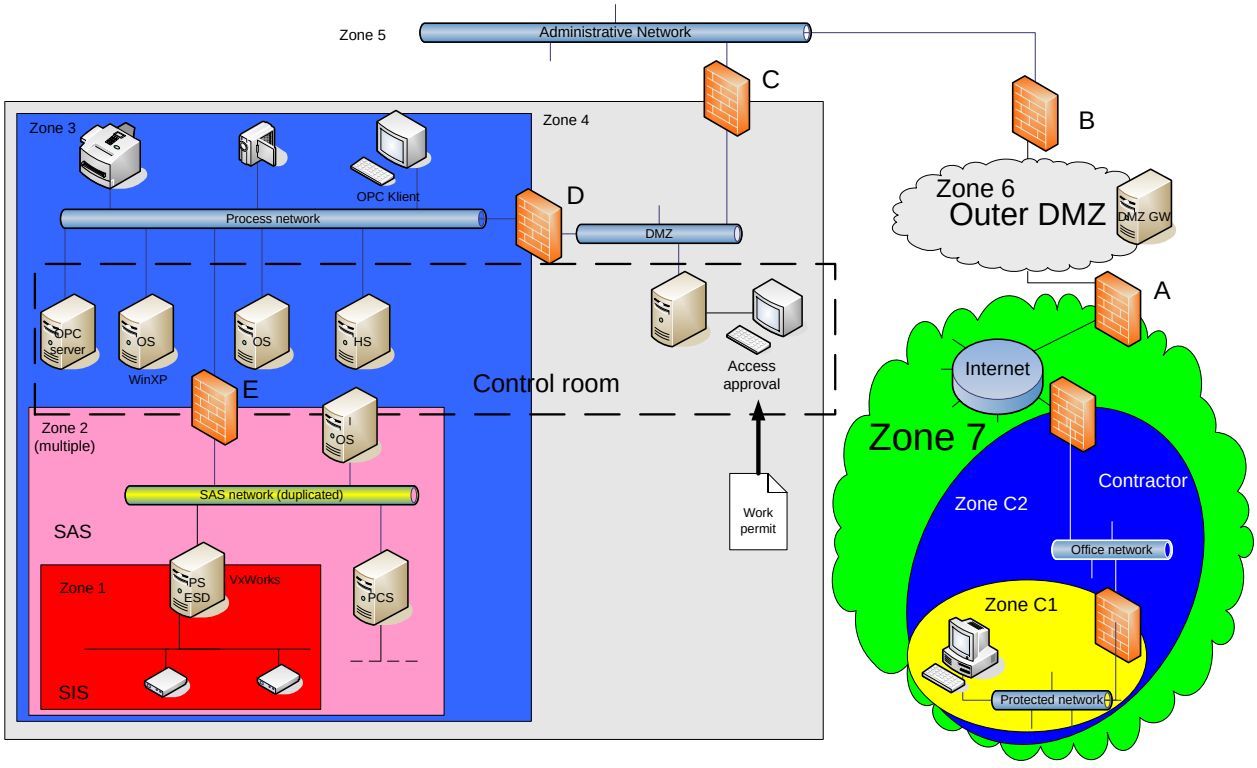


**Figure 9: Case for remote access**

The DMZ GW represents the access control mechanism that is placed in the outer DMZ (zone 6).

#### 5.4.1 Barriers between zones

Barriers between zones 7-2 are implemented using firewalls A-E. There is no separate barrier between SAS and SIS; this implies that the barrier(s) is (are) represented by the command interface offered by the units that straddle the zone boundary, e.g. the ESD. To access the ESD user interface, a remote user must as a minimum authenticate to both the "access approval" application, as well as conventional authentication to log onto the OS.

If the protection against i.e. PCS access to the ESD is insufficient, accessing the PCS is also critical.

Firewall E is shown as a barrier between the process network (zone 3) and SAS (zone 2);

### 5.4.2 Security mechanisms in individual zones

**SIS (Zone 1)**:

- All PS units must be stripped of unnecessary functionality ("system hardening")

**SAS (Zone 2)**:

- All PCS units must be stripped of unnecessary functionality ("system hardening")

**Process network (Zone 3)**:

- All OS units must be stripped of unnecessary functionality ("system hardening")
- Logon verified by domain controller
- Restricted traffic from this zone to zone 2 by firewall

**Inner DMZ (Zone 4)**:

- Strong authentication

**Administrative network (Zone 5)**:

- Domain controller for access to network resources
- General computer security measures (out of scope for this report)

**Outer DMZ (Zone 6)**:

- Access control on various levels;
    - The general public
    - Guests/contractors
    - Own employees

### 5.4.3 Read-only status server – Diode solution

It is possible to configure a read-only status server as illustrated in Figure 10. This is a solution that enables the transmission of data from one zone to a higher zone, while guaranteeing that this specific communication channel cannot be used for communication in the reverse direction. This can e.g. be implemented as a special device sending UDP[12] data enhanced with extra integrity checksum, ensuring that the receiver has significantly higher bandwidth capacity than the sender, etc. Since UDP does not acknowledge each packet, it is possible to create a device that physically only can transmit information in one direction, e.g. by cutting the "receive" wire on an Unshielded Twisted Pair (UTP) cable[13]. No messages whatsoever will be able to pass into the SAS network via this device.

The diode solution contributes to the "principle of least privilege", since it ensures that personnel who only need read access to data have no opportunity to insert data into SAS (or SIS). If a diode solution is *not* implemented for such access, all read accesses must be treated as potential write accesses, and subjected to the same stringent controls as specified for operations that perform changes to SIS/SAS configuration.

[12] User Datagram Protocol – the connectionless (unacknowledged) counterpart to TCP (Transmission Control Protocol) in the TCP/IP protocol suite.

[13] Note that due to link status verification mechanisms in network components, additional adjustments may have to be performed, e.g. connecting the severed wire to a power source to emulate a regular connection.

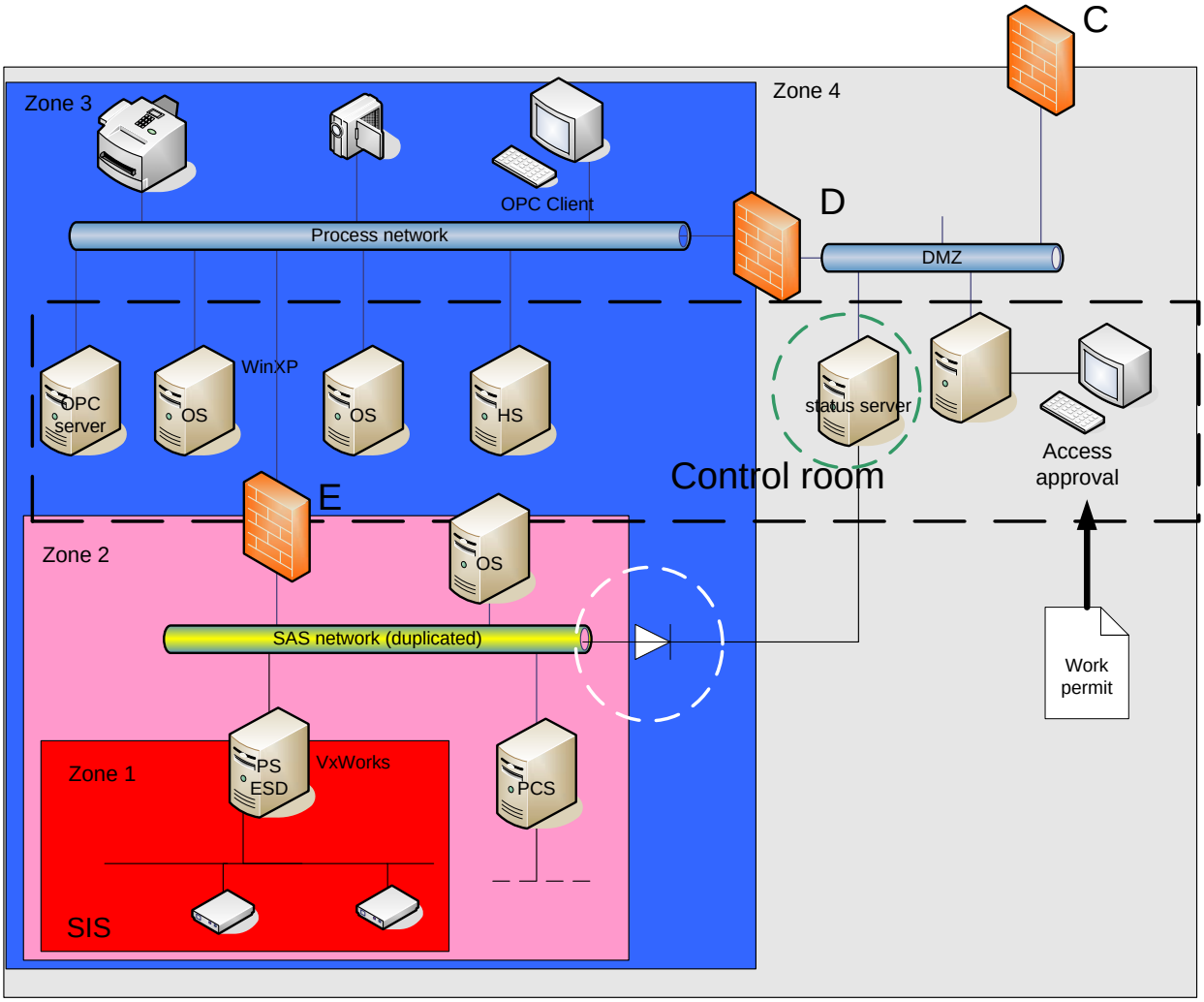


**Figure 10: Introduction of information diode for read-only access**

The status server is here placed in the inner DMZ based on the premise that the operator will want to retain a certain control over who gets access to this information, and also takes into account that having a single centralized status server for all operations, is likely to introduce too long delays in the system. Having said this, technically there should be nothing to prevent the status server from being placed e.g. in a given installation's administrative network (i.e. on the outside of Firewall C), if this is more in line with the operator's requirements.

Ideally, the status server should receive every conceivable piece of data obtainable in the Process/SAS/SIS networks. It must be determined whether this is practically possible, e.g. a new unit may be introduced that is capable of querying every valve, sensor, etc., and push this information through the diode to the status server. The bandwidth requirements must be assessed based on the size of the total data to be monitored.

### 5.4.4 Inner DMZ Proxy Functionality

In addition to providing a read-only status server, a finer granularity in access control can be achieved by not granting full "remote desktop" access to an OS, but rather having a special-purpose application running in the DMZ (e.g. on the terminal server) which contains options for executing specific operations on SAS (and SIS) devices. Taken to its ultimate conclusion, this idea would imply having a large number of distinct applications to which contractors would be granted time-limited access by use of the work permit access approval regime illustrated in Figure

10 and Figure 9. This would in effect implement the “least privilege” principle, ensuring that a given user only can execute exactly the operations that the user needs to fulfil his/her task.

It would also be possible to create a single, big “granular access” application, but that would require a separate interface for configuring access rights, and such a large application would be more difficult to verify for correctness.

### 5.4.5 OPC Communication

A common way of transferring process control information is by the use of the “OLE for Process Control” protocol. OPC was designed for communication over local area networks, which has created a demand for OPC tunnelling solutions when OPC data needs to be transferred from one process network to another. OPC tunnelling is primarily a bundling-unbundling[14] operation, and has no added security value as such. Specifically, there is no confidentiality or integrity protection of the tunnelled data.

Based on the dubious security property of OPC, we consider an OPC tunnel between two process networks to be an implicit (machine-machine) interconnection of these two networks. Furthermore, it is important that the tunnel is protected against unauthorised modification or disclosure along the transmission path. This implies that the tunnel must be encrypted, and that the plaintext data must have a cryptographically strong message integrity check added before encryption.

Even though newer equipment frequently has incorporated OPC server/client functionality, a configuration that enables a PS to establish OPC communication with any PS in a different installation should be discouraged. This can be regulated using firewall E.

[14] I.e., taking data from several connections and sending them over the internet as a single, unified connection – much like collecting numerous single subscriber telephone cables in one big multi-strand cable that goes to the telephone exchange. An OPC tunnel will on the network level appear to be a single connection, while in reality it contains multiple connections.

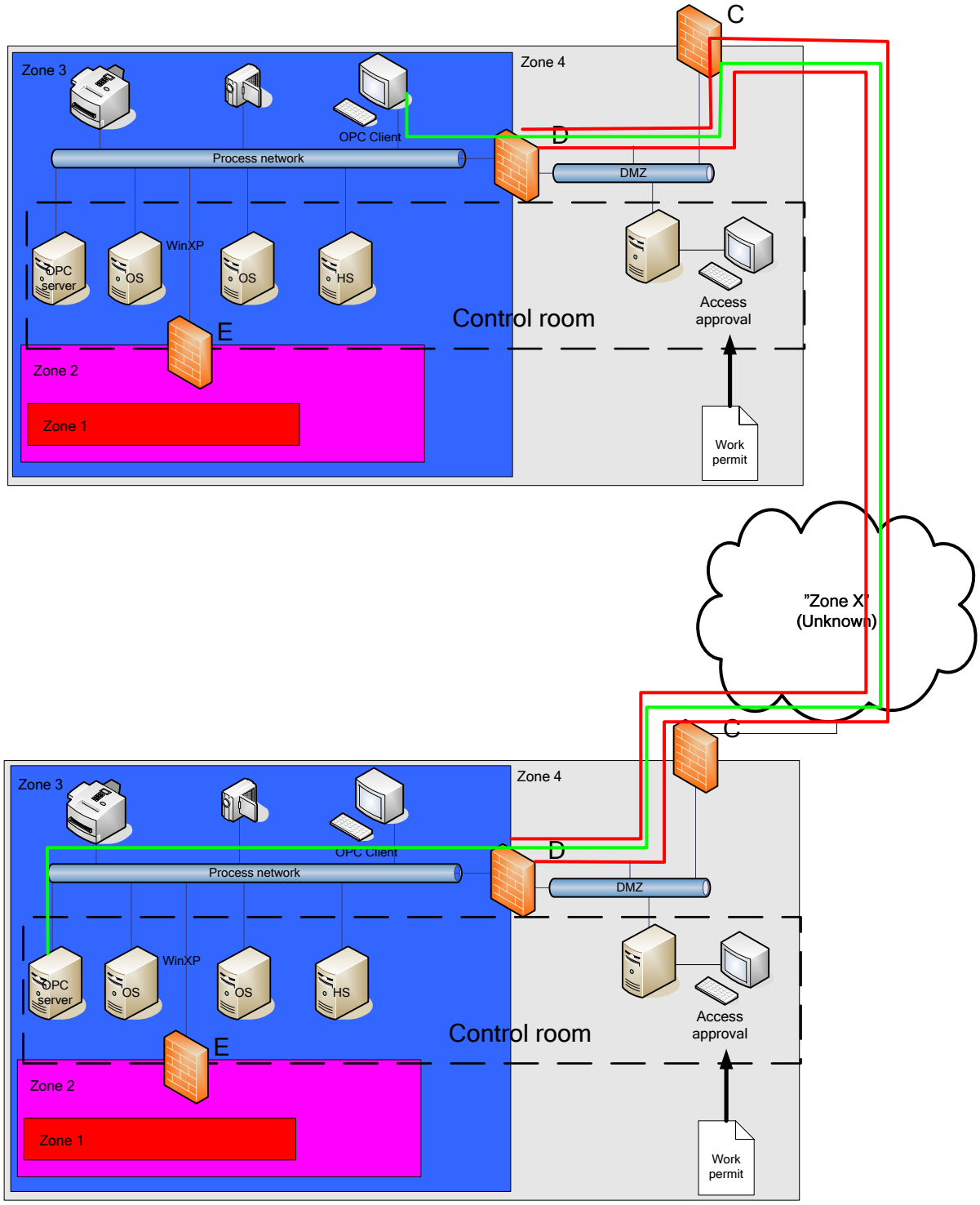


**Figure 11: OPC tunnelling between different process networks**

Since it is not known beforehand where an OPC tunnel will go, it must be assumed (as a "worst case") that it also passes through the open internet at some point between the two process networks. This is illustrated by the unknown "zone X" in Figure 11.

# 6 Example, application of the SeSa method

This chapter describes how the SeSa method may be applied by referring to the recommended system structure, detailing the standard list of threats (see Table 3), and describing a HazOp process for verifying the applicability of a chosen configuration.

## 6.1 Using the Onion Model

The layered model represents our recommendation of how a network should be structured to offer sufficient protection. For any real network, adherence with the architecture illustrated in Figure 7 and Figure 9 must be documented, and a rationale for any deviations must be offered.

Furthermore, when the network architecture has been documented to the required level of detail, the standard threats listed below must be considered, and countermeasures for each applicable threat must be documented. Any threat found not applicable for the specific network at hand must be explicitly documented as "not applicable", and the rationale must be given. Finally, a system-specific threat analysis must be performed to uncover any additional (specific) threats. All additional threats must also be appropriately mitigated.

### 6.1.1 Threats from the outside (zone 7)

a) Since integrated operations among other things assume that contractors are able to access "their" components from external networks, an intruder may be able to get illegitimate access to these same components through the contractor. E.g., if an intruder is able to plant a "remote administration tool" (RAT) such as Back Orifice in the contractor's system, the intruder may be able to access components in the inner zones by remote control.
b) If it is possible for an intruder to inject data in traffic from contractor that passes through the firewall, behaviour of the end system (the recipient of the traffic) may be altered. In extreme cases, faults such as buffer overflows may be provoked in the end systems. OPC-tunnelling is a special case of such traffic passing through the firewall(s).
c) In the case of vulnerabilities in firewall A, this may be compromised. This would allow an intruder to communicate more freely in the DMZ, but further penetration may require that the DMZ gateway and/or firewall B be compromised as well.
d) The DMZ gateway is normally by nature accessible by "anyone". In the case of a vulnerability in the former, it may be able to compromise the gateway and thus get access to both zone 6 and 5.

#### 6.1.1.1 Countermeasures

a) Strict rules regarding what kind of equipment is allowed to be used, and regarding what kind of software is allowed on this equipment. Strict filtering on which addresses the equipment is allowed to communicate with (an "allow" list rather than a "deny" list).
b) Ensure that all communication that is allowed to pass through the firewall is encrypted, and that message authentication codes (MAC) are added to the plaintext before encryption. The MAC is necessary in order to detect inserted data in encrypted traffic; encryption alone is not sufficient to prevent such insertion.
c) Continually updated and patched firewall, etc.
d) Stricter control on who is allowed into DMZ.

### 6.1.2 Threats from outer DMZ (zone 6)

a) In general, all traffic from DMZ GW is allowed through FW B; it is assumed that access is controlled by DMZ GW. A compromise of DMZ GW thus grants access to zone 5.
b) If there are other units in the DMZ that an intruder has successfully compromised, IP-spoofing may be employed if FW B performs filtering based on IP addresses (allows all

traffic originating from DMZ GW's IP address to pass through). Otherwise (if spoofing is not possible), the intruder must first compromise DMZ GW or FW B to advance further.

#### 6.1.2.1 Countermeasures

a) Need mechanisms to detect compromise of DMZ GW
b) Need mechanisms to detect spoofed IP addresses. Alternatively, encryption/MAC can be employed to ensure traffic comes from DMZ GW (may need to elaborate).

### 6.1.3 Threats from administrative network (zone 5)

a) Insiders in administrative network can inject data in traffic from contractors
b) Malware with back doors

#### 6.1.3.1 Countermeasures

a) Partially mitigated by access control/authorization. Physical topology of network, switches etc. should ensure that "pass through" traffic is not visible to ordinary users of the administrative network. Encryption/MAC of such traffic will prevent injection of data.
b) If a RAT finds its way into a client computer, an intruder will be able to observe and do anything the legitimate user can. Need mechanisms to detect malware, possibly also detection mechanisms to discover "suspicious" communication patterns.

### 6.1.4 Threats from inner DMZ (zone 4)

The threats here are mostly analogous to the threats to the outer DMZ, the only difference being that only users that are authorised in zone 5 are allowed into the inner DMZ.

a) In general, all traffic from DMZ GW ("access approval") is allowed through FW D; it is assumed that access is controlled by DMZ GW. A compromise of DMZ GW thus grants access to zone 5.
b) If there are other units in the inner DMZ that an intruder has successfully compromised, IP-spoofing may be employed if FW D performs filtering based on IP addresses (allows all traffic originating from DMZ GW's IP address to pass through). Otherwise (if spoofing is not possible), the intruder must first compromise DMZ GW or FW D to advance further.

#### 6.1.4.1 Countermeasures

a) Need mechanisms to detect compromise of DMZ GW
b) Need mechanisms to detect spoofed IP addresses. Alternatively, encryption/MAC can be employed to ensure traffic comes from DMZ GW (may need to elaborate).

### 6.1.5 Threats from process network (zone 3)

a) Units with undetermined security configuration is introduced between the networks (zone 2 and 3)
b) Equipment with valid access to zone 2 is used for accessing "dubious" networks/systems/websites
c) OPC server is compromised by external OPC server/client, and used to attack OS, HS etc. Can also compromise other OPC servers at other installations

#### 6.1.5.1 Countermeasures

a) Strict configuration control and work permits for connection equipment
b) Reduced service selection on the equipment (no web browser, e-mail client, etc.). If users are likely to "demand" these kinds of services, a strictly controlled terminal server (e.g. Citrix) could be an option (no local disk access, etc.).
c) Plug "OPC hole" by requiring encryption/authentication of all OPC tunnels. Strict configuration control on OPC tunnels

#### 6.1.6 Threats from SAS (zone 2)

a) A unit containing errors or malware may overload the ESD with data, causing it to malfunction (DoS)
b) A compromised unit in SAS is used to attack SIS.

##### 6.1.6.1 Countermeasures

a) The ESD must be constructed such that it isolates itself from external communication in the case of overload, it must still be able to execute its safety function.. If this is not possible, it shall enforce a safe state (e.g. shutdown):
b) Equipment in SAS must be configured such that all unnecessary functionality is removed (hardening).

### 6.2 HAZOP

The formal requirements to the “Hazop”-like use of the SeSa method are minimal. The main requirement is that the method is exercised by a group of professionals with combined safety and security competence and that they as a group are familiar with the actual installation. Further that the process is supervised by a process leader that is responsible for ensuring that threats and countermeasures are handled systematically at all levels, and that the assessment is properly documented.

# 7 Conclusion and recommendation for further work

In this report, we have established a conceptual basis for “secure safety” in conjunction with IEC 61508/61511 and the PDS method, and have proposed a method for assessing whether a given solution for remote access to SIS is “secure” or not.

In using the SeSa method, the term “secure” will be normative and conclusive on the basis of the knowledge that can be mobilized and explicated at the given moment of time that a “HAZOP” is exercised. An (epistemic) uncertainty will however always be present, especially in terms of ICT security where (revelations of) new threats and vulnerabilities emerge rather abrupt.

The proposed method has also been applied on a tentative case.

Based on this, further work need to be done along the following lines:

a. Further trial of the method on “real” cases
b. Extending the scope to broader “SAS” contexts
c. Development of schemes to update “approved” solutions in light of “new” knowledge of threats and vulnerabilities
d. Operation and implementation of the “value-chain” that is the result of a successful use of the SeSa method.

The latter is considered the most urgent. First, because of the limited scope of the SeSa method presented herein (providing a functional requirement specification), of which implementation and management across organisational borders is not included. Second, because a dynamic environment, both technically and organisationally, is expected to be a central characteristic of the Brave New World of Integrated Operations. The “value-chain” has to be re-constructed and updated rather frequently.

# Appendix A: Detailed comments on the NISCC good practice guide

In the following, text in `courier font` is taken directly (or paraphrased) from [2].

### 7.1 Implement secure architecture

- Network architecture
  - `Identify all connections to the PCS`. We interpret the requirements for PCS as also applicable to ESD. It is important to ensure that the only connections are the ones actually documented.
  - `Reduce the number of connections to the PCS, ensure valid business case for remaining connections`
  - `Segregate or isolate PCS from other networks.`
    E.g. process network and technical subnet. Separation of PCS and ESD in separate Virtual LANs (VLANs) should be considered, although a traditional VLAN does not offer "hard" security. Consider removing TCP/IP connections between ESD and PCS, but keep in mind that this may not be possible in current configurations (this is not required in the "onion model")
- Firewalls
  - `Protect connections between PCS and "other systems" with FW&DMZ`
  - `Deploy FW with tightly configured rule bases` – e.g. if a Citrix-like terminal server is the basis for access, only ICA-traffic should be allowed. OPC tunnelling is a special case that may warrant extra attention. More information is available in [3].
  - `Regular review of FW configuration`
  - `Strict change control of FW changes`
  - `Implement appropriate FW management and monitoring regimes – competent administrators and 24/7 duty rosters are a must.`
- Remote access
  - `Maintain inventory of all remote access connections and types`
  - `Ensure valid business justification` – "it's always been done this way" is not a justification.
  - `Appropriate authentication, e.g cryptographically strong authentication`
  - `Regular audits to exclude unauthorised connections`
  - `Procedures/Assurance for enabling/disabling connections`
  - `Restrictions: specific machines, specific users, specific times`
  - `Reviews of all third parties with access to PCS/ESD`
  - `Ensure that remote access computers are appropriately secured`
- Anti-virus
  - `Protect (SIS/PCS) system with A-V SW`
    This may be difficult with respect to the Process Station
  - `Obtain accreditation and configuration guidance from PCS/ESD vendor prior to deployment`
- E-mail and Internet access
  - `Disable e-mail and Internet access from PCS/ESD`
    Remove email clients and web browsers from Operator Stations (an alternative that may be considered is to allow Citrix-like access). Tightly configured firewalls may deny access to all sites that are not explicitly allowed.

- System hardening
  - Hardening of PCS/ESD to prevent network based attacks. Remove or disable unused services and ports in the operating systems and applications to prevent unauthorised use.
    This relates to e.g. Windows installation; more fundamentally, it may be considered if special stripped-down versions of the operating system are available. Examples of software that should be removed include Internet Information Server (web server) and telnet server (remote access). It is recommended to use separate Operator Stations specifically for remote access; these should be particularly tightly configured. Hardening also includes removing/disabling all unnecessary user accounts on a system.
  - Ensure that all inbuilt security features are enabled.
- Backups and recovery
  - Ensure that effective backup and recovery procedures are in place, and are appropriate for the identified threats. Review and test regularly
  - Test the integrity of backup recovery regularly – note that if backups are not verified, history teaches us that there is a good chance that they are worthless when you finally need them.
  - Store backups at on- and off-site locations – at the very least, there should be a recent backup set stored in a zone that is functionally separate from the operating environment
- Physical security of PCS equipment, networks etc
  Keep in mind that access to offshore installations is by definition restricted.
- System monitoring
  - Monitor behaviour and compare to ”normal baselines” in order to detect unusual behaviour (e.g. network monitoring to detect worms)
  - Intrusion detection tailored to the PCS environment
  - Review and analyse log files regularly
  - CCTV, Tamper alarms: especially important for ”really remote”
  - Ensure that access to secure areas via passcards is logged
- Wireless networking
  Use of wireless networks is discouraged by the good practice guide; however, it should be noted that with careful configuration an selection of encryption algorithms, modern wireless networks will offer acceptable security also for SCADA systems.
- Security Patching
  - Implement processes for deployment of security patches
  - Support by audit and deployment tools
  - Vendor certification of patches, testing of patches prior to deployment, Staged deployment to minimise risk
  - Work-arounds in cases where patching is not possible
- Personnel background checks
  This is assumed to be in place, but is outside the scope of this report.
- Passwords & accounts
  - Password policy for PCS that covers password strength and expiration times (or alternative policies)
  - Regular review and decommissioning of access rights and (old) accounts
  - (Where possible) change vendor passwords from vendor defaults

  - Password requirement may be waived for specifically defined ”read-only” access, if available.
  - Consider stronger authentication methods for critical functions
- Document security framework
  - Document full inventory of PCS (Systems and components)
  - Document the framework for PCS security (detailed about risk assessments, assumptions made, known vulnerabilities and security measures deployed)
  - Ensure all PCS documentation is secured (access limited to authorised personnel)
    However, do not base the security of the PCS on the assumption that this information remains secret.
- Security scanning
  See below.
- Starters and leavers process
  This is outside the scope of this report.
- Management of change
  - Certify that all systems are subject to strict change control processes. Security assessments shall be included. Changes may be subject to multiple change control processes, e.g. FW modification controlled both from automation and IT point of view.
- Security scanning and testing
  - Penetration testing and scanning should be carried out when possible (on dedicated test environment, on backup systems, or during shut-down)
  - All IP enabled control devices should undergo security testing to gain assurance that they are not vulnerable to common DoS attacks, but also other protocols should be tested
  - Undertake full risk assessment prior to any scanning/testing activities
- Device connection procedures
  - Establish a procedure to verify that devices are free from virus or worm infections before they are allowed to be connected to PCS networks

### 7.2 Manage third party risks

Although not checked in the table, we mention some salient points on third-party risks.

- Identify third parties, including vendors and service providers, and all other links in the supply chain that are associated with the PCS
- Manage risks from vendors
- Ensure that security clauses are detailed in procurement contracts
- Engage with vendors on an ongoing basis to ensure that any current or future discoveries of vulnerabilities are identified and notified promptly
- Request vendors to provide security guidance for their current PCS and a security roadmap for future system development
- Ensure that vendors incorporate anti-virus protection within their PCS
- Establish with the vendor an effective software patching process
- Agree with the vendor the system hardening procedures for the PCS in operation
- Undertake regular security reviews and audits of all vendors
- Manage risks from support organisations

- Undertake regular risk assessments of support organisations and ensure any countermeasures are implemented!
- Prevent access to the PCS by support organisations until appropriate measures have been implemented. Issue contract
- Are there opportunities for more “ephemeral” connections?
- Engage with support organisations on an ongoing basis to ensure that any current of future…
- Increase awareness of all support organisations to fully understand the security challenges.
- A possible major problem: Do operators offload so much responsibility on the contractors as to make these requirements “impossible”?
- Manage risks in the supply chain
- ...accordingly with ”all others” that come in contact with PCS

## Appendix B: What is a firewall?

A firewall is a network component that is capable of controlling network traffic crossing a domain boundary. Functionally speaking, a firewall can be described as a rule set that specifies what traffic is allowed to cross the boundary in which direction. In real life, a firewall may be a system ("box") that implements one or more rule sets, and thus represents one or more boundaries.

Modern firewall units have two or more network interfaces. A firewall with two NICs will typically be used to control one network boundary, and contain one rule set. The simplest form of firewall is known as a packet-filtering gateway, which applies rules on a per-packet basis. Basic packet-filtering includes the capability to accept or deny traffic based on source and/or destination address, and service types (destination and possibly source TCP port numbers). Modern packet filters are now increasingly complex, with the capability of buffering a number of network packets, performing payload inspection, and more.

Firewalls that require increased authentication, access control, and/or restriction of allowable traffic types may employ proxy services. A firewall proxy is a program (or process) that presents itself to the outside world as certain type of server (e.g. a mail server). It is possible for outsiders to connect to the proxy and issue the same commands and data as one would to the server, but apart from possibly filtering the data in various manners, the proxy does not process the data itself, but rather passes it on to the real server, hidden behind the firewall. In this way it is possible to "sanitize" the data that is passed through to the server; any data that the proxy doesn't understand will be discarded. Note that a proxy program will be much less complicated than the server it acts on behalf of, and it is thus much easier to ensure secure operation of a proxy than the server itself.

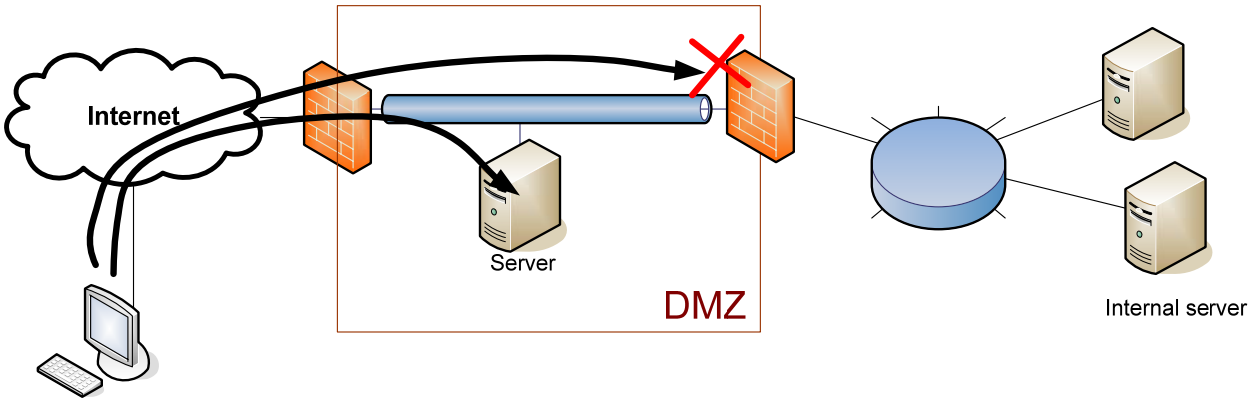


**Figure 12: DMZ concept**

Many firewall configurations include a so-called De-Militarized Zone (DMZ), as illustrated in Figure 12. The idea behind a DMZ is to place publicly available servers on a separate subnet, protected from the internet by a firewall (rule set). In the figure, the leftmost firewall will allow traffic from the outside client to reach the server, but will block any attempts to communicate with other units, e.g. the rightmost firewall. In many cases, the server in the DMZ will need to communicate with resources in the internal, protected network far right in the figure. It is then the responsibility of the rightmost firewall to ensure that only traffic originating from the DMZ server is allowed through to the internal network. A DMZ may be realized by employing two separate dual-homed firewalls, or a single firewall with three network interfaces.

The DMZ is the logical place to position a public web server or a remote access facility.

More detailed information on firewall technology can e.g. be found in [29].

## References


[1] Norwegian Petroleum Directorate “Forskrift om styring i petroleumsvirksomheten (Styringsforskriften)” §1, December 2004

[2] NISCC Good Practice Guide – Process Control and SCADA Security, PA Consulting Group, October 2005

[3] Good Practice Guide – Firewall Deployment for SCADA and Process Control Networks. NISCC, UK. 2005 . http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf

[4] Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, NIST special publication 800-82 (initial public draft), September 2006 http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf

[5] T.O. Grøtan. *Secure Safety in Remote Operations*. ESREL 2006, Estoril, Portugal

[6] T. O. Grøtan and M.G. Jaatun: *Secure Safety*, presentation at PDS forum, Trondheim, April 5th 2006 (in Norwegian)

[7] E. Schoitsch: “Design for safety and security of complex embedded systems: A unified approach”, in “Cyberspace Security and Defense: Research Issues”, Gdansk 6-9 September 2004, NATO Science Series II - Mathematics, Physics and Chemistry, Vol 196

[8] K.T. Kosmowski, M. Sliwinski & T. Barnert: “Functional safety and security assessment of the control and protection systems” . ESREL 2006, Estoril. Portugal

[9] M. Howard and D. E. Leblanc, Writing Secure Code. 2. ed. Microsoft Press 2002

[10] A. McIntyre, A. Lanzone and J. Stamp, I3P Preliminary Risk Characterization Report, 13.03.2006 available: http://www.thei3p.org/about/researchreport6.pdf

[11] Auguste Kerckhoffs, La cryptographie militaire, Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.

[12] OLF Guideline 104 “Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems”, 2006. see http://www.olf.no/?35820.pdf

[13] Bundersamt für Sicherheit in der Informationstechnik: *IT Grundschutz Manual* http://www.bsi.de/english/gshb/manual/

[14] Brown, J.S. and P. Duguid. “Enacting Design for the Workplace.” In Adler, P.S., and T.A. Winograd. “USABILITY. Turning Technologies into Tools”. Oxford University Press. 1992

[15] Committee on Information Systems Trustworthiness: “Trust in Cyberspace.” National Research Council (USA). http://stills.nap.edu/html/trust/index.htm

[16] US Department of Defense “Trusted Computer System Evaluation Criteria”. 1987 Washington DC

[17] Garfinkel, S. C., F. Lorrie. “Security and Usability”. O’Reilly. 2005

[18] Line, M.B, O. Nordland, L. Røstad, I.A. Tøndel. ”Safety vs Security?”. Paper presented at the 2006 PSAM conference, New Orleans, USA

[19] Naedele, M. “Standardizing Industrial IT Security – A first look at the IEC approach” http://www.tik.ee.ethz.ch/~naedele/etfa05.pdf

[20] NRC 2006 http://www.forskningsradet.no/petromaks

[21] PDS 2006 http://www.sintef.no/static/tl/projects/pds/www/

[22] IEC 61508 Functional safety of E/E/PE safety-related systems

[23] IEC 61511 Functional safety – Safety Instrumented systems for the process industry sector

[24] ISO 15408 Information technology - Security techniques - Evaluation criteria for IT security (see also http://www.commoncriteriaportal.org/)

[25] ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, 2005

[26] Randi Røisli: ” Uønskede hendelser, oppfølging mot indikatorer og planer videre” presentation at ”HMS og IKT-sikkerhet i integrerte operasjoner”, Stavanger, November 29th 2006
[27] Jens Kristian Engstrøm / Harald Hilde: ” Remote operation and security – experiences from a Power Utility”, presentation at ”HMS og IKT-sikkerhet i integrerte operasjoner”, Stavanger, November 29th 2006
[28] Robert Malmgren: ”SCADA and process control security” presentation at “Arbeidsseminar om IKT-sikkerhet og Integrerte Operasjoner” Stavanger November 30th 2006
[29] G. Hallingstad, M.G. Jaatun and R. Windvik: “Firewall Technology”, FFI/PUBLICATION-2002/01741, Norwegian Defence Research Establishment 2002
[30] OLF Homepage on Integrated Operations; www.olf.no/io
[31] Stamp Jason, John Dillinger, William Young, and Jennifer DePoy. November 11, 2003. "Common Vulnerabilities in Critical Infrastructure Control Systems", Sandia National Laboratories, 2nd edition. Available at http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf
[32] CORAS risikoidentifikasjon. Foredrag av Erik Wisløff, Telenor FoU, http://www.sintef.no/static/td/arr/mars2004/presentasjoner/risk-identification.pdf

Technology for a better society

**www.sintef.no**