Secure Safety: Secure Remote Access to Critical Safety Systems in Offshore Installations

Martin Gilje Jaatun[1], Tor Olav Grøtan[2], and Maria B. Line[1]

[1] SINTEF ICT
[2] SINTEF Technology and Society
{Martin.G.Jaatun,tor.o.grotan,maria.b.line}@sintef.no

Abstract. Safety Instrumented Systems (SIS) as defined in IEC 61508 and IEC 61511 are very important for the safety of offshore oil & natural gas installations. SIS typically include the Emergency Shutdown System (ESD) that ensures that process systems return to a safe state in case of undesirable events. Partly as a consequence of the evolving "Integrated Operations" concept, a need is emerging for remote access to such systems from vendors external to the operating company. This access will pass through a number of IP-based networks used for other purposes, including the open Internet. This raises a number of security issues, ultimately threatening the safety integrity of SIS.

In this paper we present a layered network architecture that represents current good practice for a solution to ensure secure remote access to SIS. Also, a method for assessing whether a given solution for remote access to SIS is acceptable is described. The primary objective with the specification of the remote access path is to defend the Safety Integrity Level (SIL) of SIS from security infringements. It also accommodates the special case when security functions have to be implemented within SIS.

Keywords: Process Control, Offshore, Secure remote access, Safety Instrumented Systems.

1 Introduction

The concept of Integrated Operations (IO) is emerging as the preferred way of working in the oil and gas industry. Real-time cooperation between on- and offshore staff is required in order to optimize production, and new technologies and new work processes enable this.

Commercial-off-the-shelf (COTS) hardware and software and Internet connections are among the new technologies introduced, where "new" means that they have not been widely used in the context of process control before. The application area is remote operation, which enables onshore staff to log on to, and perform operations on, process control systems (PCS) and Safety and Automation Systems (SAS) offshore. This opens for a whole new set of threats related to information security that need to be considered.

Safety Instrumented Systems (SIS) are crucial subsystems offshore. According to the IEC 61508/61611 series of standards [1] [2] and the PDS method [3],

C. Rong et al. (Eds.): ATC 2008, LNCS 5060, pp. 121–133, 2008.

they are of paramount importance for the safety of an offshore installation. SIS typically include the Emergency Shutdown System (ESD), which often is the ultimate guarantor for fail-safe properties at such installations.

The use of new technologies must be trusted to not have any negative impact on SIS; i.e. impact that could raise significant doubt on its claimed Safety Integrity Level (SIL) [1]. This means that the communication channels used during remote operations must be technically secure, such that they can not be tampered with, misused or in other ways used to compromise SIS.

Information security is usually defined by the three terms confidentiality, integrity and availability [4]. In this paper the scope is limited to integrity concerns for SIS, which means that the objective of the "good practice for remote access" is to prevent unauthorized changes to SIS.

Industrial safety and information security issues are two related – but still rather different – fields of theory and practice [5]. In some application areas it is useful to seek to combine the two, and process control is an example of such an area. Combination will not be unproblematic, and some problems are already manifest in the mixed vocabulary that needs to be employed when we are addressing safety and security, respectively. Practitioners within both fields are concerned about this challenge. As further discussed in [6], combining these two approaches into a coherent whole is not achieved solely through a technical report, but a modest hope is that this paper may contribute to such a development.

In this paper, a network topology for secure remote access to SIS is presented. The solution includes contractor's network, operator's office network and process control network, and security mechanisms. Also, a method is described that can be used to assess whether a given network solution for remote access to SIS is acceptable. The paper is based on results from the Secure Safety (SeSa) project, funded by the Norwegian Research Council and PDS Forum.

The remainder of this paper is structured as follows: Section 2 refers to related work, and our research method is briefly described in section 3. The good practice network topology is presented in section 4 and section 5. The method for assessing the impact on SIL is described in section 6. We give our conclusion in section 7 and suggest further work in section 8.

2 Related Work

The background and approach for the SeSa project was documented in [7]. Line et al. [5] discuss general challenges in considering both safety and security in a given situation. Schoitsch [8] and Kosmowski et al. [9] explore relationships between traditional "security" assurance and "safety assurance" as exemplified by SIL.

The UK Centre for the Protection of National Infrastructure (formerly NISCC) has published guidelines on security of SCADA systems in general [10], and on firewall deployment in such networks in particular [11]. The US National Institute of Standards and Technology (NIST) has also released a preliminary guide to SCADA security [6]. Naedele [12] presents insights on IEC standardization efforts in industrial IT security, although it does not appear that the IEC today is any closer to a finalized standard.

The Norwegian Oil Industry Association (OLF) has published a set of Information Security Baseline Requirements [13] which all operators on the Norwegian Continental Shelf eventually will have to comply with.

The SeSa project has not significantly extended the good practices mentioned above, but ventures to combine them into a coherent whole for the specific case of secure remote access to SIS.

3 Method

The SeSa project studied a small number of Norwegian offshore operators and contractors, and participated in two sessions of PDS Forum in 2006 [3]. The PDS Forum meetings have a broad participation of experts from the Norwegian process control community.

The interviews and the PDS Forum discussions contributed to the survey on how the communication networks are implemented today within the process control domain. This includes the operator's office network, the contractor's network and their solutions for remote control, the process control systems offshore, and the security mechanisms in use. Possible improvements were then identified, based on state of the art and earlier experiences, regarding structure of the network topology and security mechanisms to be added or modified. The network topology presented in this paper therefore (in similarity with many other "good practice" efforts) represents a synthesis of how it is actually implemented in the offshore industry today and the ideal solution.

4 Structuring the Remote Access Path

A basis for ensuring secure remote operation is that the networks that constitute the remote access path are organized in a manner that adheres to the principle of "defense in depth"[1], and that suitable access control mechanisms are employed.

4.1 The "Onion Model"

The left side of Fig. 1 depicts a layered access model from an operator's point of view. This model is based on two demilitarized zones (DMZ); one serving as a buffer between the operator's network and "the outside world", while the 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).

[1] This is the opposite of the "Maginot line" principle of relying on a single point of failure.

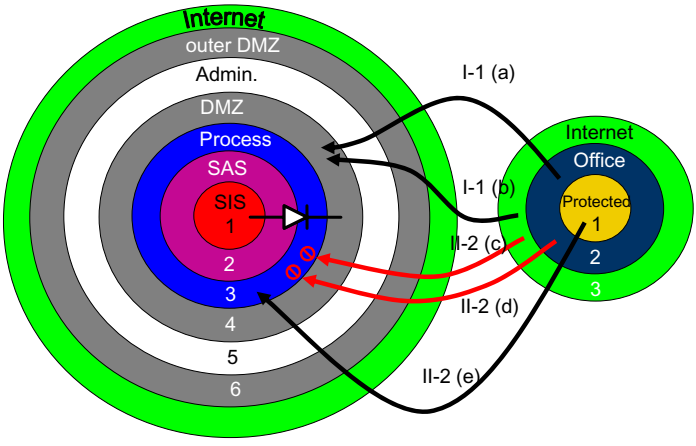

Fig. 1. Layered model with allowed and rejected access attempts

The layered model of Fig. 1 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 [14]. Furthermore, the separation of the process network from the administrative network is as recommended in the NISCC good practice guide [10]. 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 the right side of Fig. 1, where equipment used to access the operator's network is placed in a zone separated from the general office network. Note that since access in this model conceptually always originates from the contractor, there is no need from our point of view for the contractor to have a DMZ between its office network and the internet - a single barrier (i.e. firewall) is sufficient. This is also illustrated in Fig. 2.

4.2 Threats and Countermeasures

As part of the SeSa method, we have compiled a list of common threats and countermeasures that are applicable to the access model in Fig. 1. This list is based on sources like [15] and [10]. Space does not permit the reproduction of the full list here, but identified threats originating from "the outside" (zone 7) are listed in Table 1. The physical configuration suggestion that is described in the following sections represents a response to the identified threats and necessary countermeasures.

We have as a rule described the threats as originating from an adjoining zone, but the ultimate goal for a given attack may be to traverse all interfaces to affect

Table 1. Threats originating from zone 7

From Zone	To Zone	Threat	Ultimate impact on zone	Countermeasure
7	c1	Attack on contractor's zone 1	1	Configuration control, administrative measures (Specifically: Not allowed to access c1 from c2), Firewalls and c1 tightly configured, hardened
		Malware planted in contractor's "secure zone"	1	Configuration control, administrative measures
7	7	Manipulation of legitimate traffic	1	Encrypt and authenticate
7	6	Attack on firewall A	6	Firewalls must be tightly configured and patched
		Attack on other resource in zone 6	6	Don't have other resources in DMZ, Other resources that have to be in the DMZ must be tightly configured (hardened)
7	6	Attack on DMZ gateway	5	Tight configuration and hardening, Strong authentication, Restrict access to DMZ GW to pre-defined addresses

the innermost zone, e.g. in order to illegitimately shut down an oil installation[2]. Note that no pre-compiled list of threats can ever be considered "complete" for any real networked system; the threats we have identified 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 [16], and assume that an attacker has access to all pertinent information regarding a system (network topology, configuration) *except* passwords, encryption keys, etc.

4.3 Access Modes

If a substantial part of the need for remote access is to read status information without making any changes, it is strongly recommended to consider a technical solution that offers such "read only" access (see 5.1). A "read-only" solution will in itself be easier to verify 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, thus increasing the chance for

[2] From a safety point of view, the threat would have been the reverse, i.e., *preventing* a necessary shutdown from taking place.

success in the "1st round" in Fig. 3. Furthermore, a read-only solution may also potentially be reachable from a wider (looser) set of operational contexts on the vendor side, as indicated in Fig. 1.

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

These can be further refined as shown in Table 2.

Table 2. Access modes

I-1	Snapshots of SIS state (via "information diode" - see section 5.1). 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 Process Station (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

4.4 Access Examples

The various access options described in section 4.3 can now be mapped to the layered models as illustrated by the arrows in Fig. 1, where it is assumed that "information diode" functionality (see 5.1 for details) is available.

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 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.

4.5 Physical Mapping

An example of how the layered "onion" models presented above may be translated into a physical network configuration is presented in Fig. 2. 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.

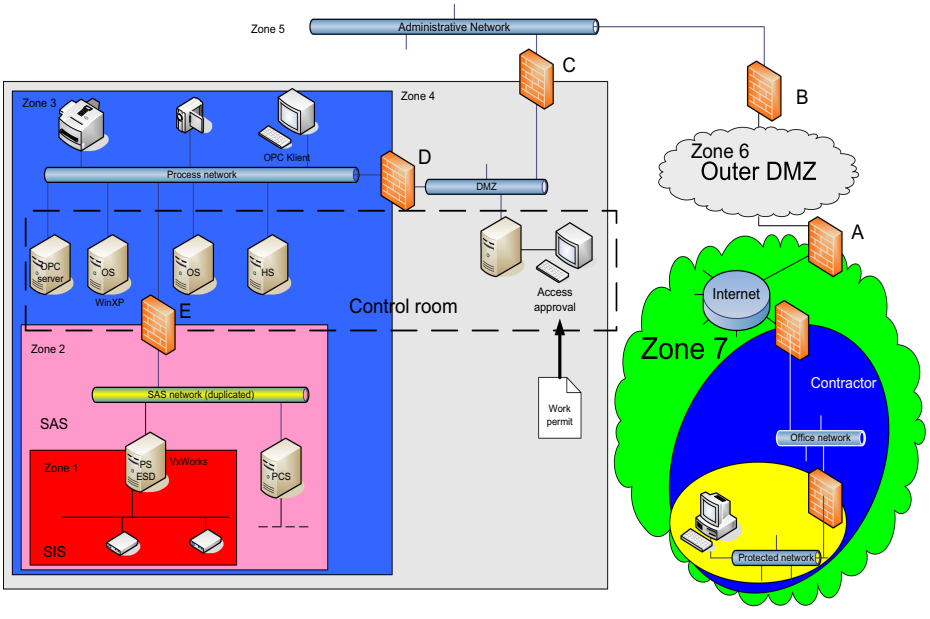

Fig. 2. Case for remote access

We repeat that although not shown explicitly, some sort of access control mechanism is assumed to be placed in the outer DMZ (zone 6).

4.6 Barriers between Zones

Barriers between zones 7-2 are implemented using firewalls A-E. Additionally, there is a manual "access approval" application in the inner DMZ (zone 4), where an operator can grant (or deny) access attempts originating e.g. from onshore contractors. Technically, this may be implemented as part of a terminal server application. Good practice would in this case indicate that all such accesses should be in accordance with a formal work permit.

There is no separate barrier between SAS (Safety and Automation System) 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 Operator Station.

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); it may also serve as a barrier between different SAS segments (if appliccable).

4.7 Security Mechanisms in Individual Zones

As a rule, equipment in the inner zones exhibit "special purpose" properties to a greater extent than equipment in the outer zones. Thus, the equipment in the inner zones also generally has fewer configurable security mechanisms.

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 Operator Station (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 paper)

Outer DMZ (Zone 6)**:**
- Access control on various levels;
  - The general public
  - Guests/contractors
  - Own employees

4.8 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 frequently merely a bundling-unbundling operation, in which case it 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 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.

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.

5 Additional Mechanisms

In the previous section, recommendations for structuring the remote access path were described. In certain situations, it may be possible to further mitigate a large number of threats by architectural choices. Two such options are described below.

5.1 Read-Only Status Server

It is possible to configure a read-only status server e.g. by connecting a special device (which we can call "information diode") between the Safety and Automation System and a status server in the inner DMZ. The information diode can be realized by sending UDP 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[3]. There are also commercially available products (e.g. [17]) that offer this functionality.

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 D), 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.

[3] Of course, there are a few more practical problems that must be solved in an implementation of this concept - which also explains why there are commercial alternatives available.

5.2 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 Operator Station, 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 Fig. 2.

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.

6 The SeSa Method

Use of the SeSa method on a given case is illustrated in the flow-chart of Fig. 3. In short, the method comprises the following steps:

1. Establish overview of threats and known weaknesses
2. Develop requirements specification of the "security value chain" [7] for the remote access path
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 (first round)
5. If impact still cannot be ruled out, identify additional security functions within SIS, and assess through HAZOP whether this will provide sufficient

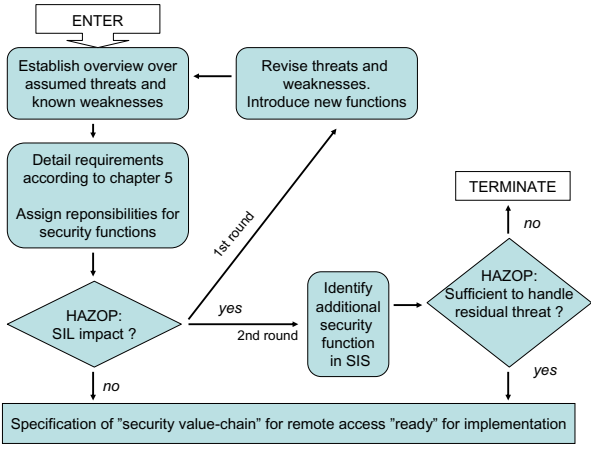

Fig. 3. The SeSa method

protection vs the residual threat (second round). 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

6. If "success" is not achieved after the second round, the proposed solution should be discarded.

The HAZOP (Hazard and Operability Analysis) [18] technique is frequently used and well-established in industrial safety. In the SeSa method we use HAZOP to identify threats and verify whether these threats are mitigated by the proposed design of the remote access path. 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, 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.

It may be difficult to gauge the assurance consequences of adding a COTS component to a system that has a given SIL. Kosmowski et al. [9] argue for a mapping between SIL and Common Criteria Evaluation Assurance Levels (EAL) [19]. However, it should be noted that a given EAL only says something about our assurance that the mechanisms defined in the appropriate Protection Profile have been properly implemented; if these are insufficient to guarantee our desired SIL, a mapping between EAL and SIL is meaningless. On the other hand, if the mechanisms we rely on to provide our given SIL is included in the component's Protection Profile, we believe that the mapping proposed in [9] may be appliccable.

7 Conclusion

In this paper, we have presented good practice for secure remote access to Safety Instrumented Systems in an offshore process control system. Furthermore, we have introduced the *SeSa method* for assessing whether a given network solution is acceptable when it comes to ensuring the integrity of SIS.

The network solution presented complies with advice and guidance given by several actors in the industry. This fact contributes to assurance that the solution is acceptable and ensures an appropriate level of security for SIS.

8 Further Work

Further work needs 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.

Acknowledgments

This paper has presented results from the SeSa research project funded by the Norwegian Research Council and PDS Forum. We are grateful for the participation of Tor Onshus (NTNU), Knut Øien (SINTEF T&S), Stein Hauge (SINTEF T&S) and all PDS Forum attendees.

Also thanks to Odd Nordland, SINTEF ICT, who made helpful comments on a previous version of this paper.

References

1. Functional safety of E/E/PE safety-related systems, IEC Std. 61 508 (1998)
2. Functional safety - Safety Instrumented systems for the process industry sector, IEC Std. 61 511 (2003)
3. The PDS webpage. Visited, 2007-03-09, http://www.sintef.no/static/tl/projects/pds/www/
4. Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC Std. 27 001 (2005)
5. Line, M.B., Nordland, O., Røstad, L., Tøndel, I.A.: Safety vs Security?. In: Proceedings of PSAM 8, New Orleans (2006)
6. 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
7. Grøtan, T.O.: Secure Safety in Remote Operations. In: Proceedings of ESREL 2006, Estoril, Portugal (2006)
8. Schoitsch, E.: Design for safety and security of complex embedded systems: A unified approach. In: Cyberspace Security and Defense: Research Issues. NATO Science Series II - Mathematics, Physics and Chemistry, vol. 196 (2006)
9. Kosmowski, K., Sliwinski, M., Barnert, T.: Functional safety and security assessment of the control and protection systems. In: Proceedings of ESREL 2006, Estoril, Portugal (2006)
10. NISCC Good Practice Guide - Process Control and SCADA Security, PA Consulting Group on behalf of NISCC, Tech. Rep. (October 2005), http://www.cpni.gov.uk/docs/re-20051025-00940.pdf

11. Byres, E., Karsch, J., Carter, J.: Good Practice Guide - Firewall Deployment for SCADA and Process Control Networks. British Columbia Institute of Technology, on behalf of NISCC, Tech. Rep. (2005), http://www.cpni.gov.uk/docs/re-20050223-00157.pdf
12. Naedele, M.: Standardizing industrial IT security - a first look at the IEC approach. In: Proceedings of 10th IEEE Conference on Emerging Technologies and Factory Automation, vol. 2, p. 7 (2005)
13. OLF Guideline 104: Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems (2006), http://www.olf.no/?35820.pdf
14. Forskrift om styring i petroleumsvirksomheten (Styringsforskriften), Norwegian Petroleum Directorate, §1 (December 2004)
15. IT Grundschutz Manual. Bundesamt für Sicherheit in der Informationstechnik (2004), http://www.bsi.de/english/gshb/manual/
16. Kerckhoffs, A.: La cryptographie militaire. Journal des sciences militaires IX, 5–38 (1883)
17. Whitepaper: Tenix Interactive Link Data Diode. Tenix America (a subsiduary of Tenix pty). Visited 2007-03-16 (2006), http://www.tenixamerica.com/images/white_papers/TenixIL_DataDiode.pdf
18. Hazard and operability studies (HAZOP studies) - Application guide, IEC Std. 61 882 (2001)
19. Information technology - Security techniques - Evaluation criteria for IT security, ISO/IEC Std. 15 408 (2005), http://www.commoncriteriaportal.org/