VATTENFALL

KEMA Limited

Vattenfall

Report on Audit of External Third Party Access for OPAL

G07-1667D007 Rev 1

26 October 2007

KEMA

Table of Contents

Table of Contents ..... **ii**

Revision History ..... **iii**

1. Introduction **1**

1.1 Background 1
1.2 Current Work 1
1.3 Scope of Document 1

2. Project Structure and Assessment Process **2**

2.1 Introduction 2
2.2 Assessment Project Team 2
2.3 Meetings 2
2.4 Comments 3
2.4.1 Assessment Project Team *3*
2.4.2 Meeting Durations *3*
2.4.3 Personnel Attending the Assessment Meetings *3*
2.4.4 Documentation Requirements *4*
2.4.5 Reusability of "Vendor End" Assessment *4*

3. Assessment Checklist **6**

3.1 Introduction 6
3.2 Comments 6
3.2.1 Relevance to "User End" and "Vendor End" *6*
3.2.2 Structure of checklist *6*
3.2.3 Content of checklist *7*

4. Electronic Security Perimeter (ESP) **8**

4.1 Introduction 8
4.2 Applying the ESP to External Third Party Access 8

Appendix A – Documentation Requirements List **1**

Revision History

Rev.	Date	Description	Author	Checker	Approver
0	15/06/07	Issued for comment.	Marc Tritschler		
1	26/10/07	Updated with Vattenfall and Siemens comments.	Marc Tritschler		

1. Introduction

1.1 Background

In March 2006, Vattenfall's Erik Sandström convened a Cigré task force to address the issue of cyber security relating to external third-party access to critical control systems (i.e., remote access to critical control systems by external support and maintenance providers). The main objective of the task force was to develop an efficient and effective approach to assist control systems users and control systems support and maintenance providers (usually the original vendors) in measuring the cyber security risk related to external third-party access.

The task force, consisting of representatives from control systems users, control systems support and maintenance providers (vendors) and industry consultants, produced a checklist to be used for examining the cyber security of external third-party access arrangements. This checklist is based on the NERC CIP standards used in North America, applied specifically to external third-party access.

1.2 Current Work

After the checklist was drafted, the task force members agreed that it should be trialled in order to gain experience in using it and to provide feedback on required and potential improvements. Erik Sandström secured the interest of Vattenfall's generation coordination centre in Sweden, and its system vendor Siemens, in participating in a trial. The generation coordination centre uses a system called OPAL for coordination of generating plant from Vattenfall's Stockholm control centre. The system is based on the Siemens Spectrum product, which in this case is supported by Siemens from their Oslo offices.

The trial involved completing an assessment using the developed checklist. This required assessment meetings with Vattenfall's personnel responsible for the IT security of the OPAL system environment in Stockholm, and meetings with Siemens personnel responsible for the provision of support and maintenance services in Oslo.

1.3 Scope of Document

The scope of this document is to document general feedback on the assessment process, and the checklist used for the assessment. This feedback can be used by Vattenfall and Cigré to further develop the checklist and the assessment process, if required.

The document does not contain any details of the results of the assessment, or the technical and commercial arrangements between Vattenfall and Siemens.

2. Project Structure and Assessment Process

2.1 Introduction

This section of the document describes the project structure and the approach used for the assessment, and provides comments on both.

The task force identified that an assessment of cyber security for external third-party access is not purely an assessment of the vendor end of the connection. Both the vendor end and the user end of the connection must be assessed in order to obtain an overall picture. For this reason, the checklist contains two assessment columns for each item: one column for the user assessment and one for the vendor assessment, and an indication of the relevance of each checklist item to both the user and the vendor. Other than this, there is no guidance about how the assessment should be carried out.

2.2 Assessment Project Team

The assessment project team consisted of three members. All three members attended all of the meetings described below. None of the three members of the project team were Vattenfall (or Siemens) personnel directly associated with the OPAL system. In this sense, the assessment project team was independent of the system and environment being assessed.

2.3 Meetings

The project was planned on the basis of three meetings as follows:

- A kick-off meeting with the assessment project team and all key project stakeholders from both Vattenfall and Siemens. This meeting was used to discuss and agree the detailed scope of the project and to secure agreement from all parties to participate. At this meeting, key questions relating to the assessment were also discussed and agreed. This was a one-day meeting.

- A “user end” assessment meeting between the assessment project team and the Vattenfall personnel responsible for the IT security of the OPAL system environment, held in Stockholm. This meeting was held over a two-day period.

- A “vendor end” assessment meeting between the assessment project team, the Vattenfall personnel responsible for the IT security of the OPAL system environment, and the Siemens personnel responsible for the provision of support and maintenance services, held in Oslo. This meeting was held over a two-day period.

2.4 Comments

2.4.1 Assessment Project Team

The assessment project team consisted of three members as described above. Whilst each member played an important role in the assessment project, for future assessments a two member team would probably be sufficient. The intensive nature of the assessment and the need to record significant amounts of information leads to the conclusion that it would not be preferred for a single assessor to undertake the assessment alone.

2.4.2 Meeting Durations

The "user end" assessment meeting was held over a two-day period and it was a significant challenge to complete the checklist in the time allowed. The main reasons for this were as follows:

- The assessment project team were just starting to build a full understanding of and familiarity with the checklist.
- Some of the terminology used in the checklist required interpretation and discussion in order to agree on how they applied to external third-party access. In particular, the definition of the Electronic Security Perimeter (ESP) required some debate and clarification in the context of this assessment. This is expanded further in section 4 of this document.

The "vendor end" assessment meeting was also held over a two-day period and the checklist was completed comfortably within the time allowed. However, the checklist could not have been completed in a single day.

In order to quickly build an appreciation of the systems, architectures and platforms concerned, the assessment team briefly toured the areas where relevant equipment was located, at both the user's offices and the vendor's offices. This was a very useful activity at the start of each of the assessment meetings.

For future assessments, the suggested time allocations are:

- Kick-off meeting – 1 day;
- "User end" assessment meeting – 2 days;
- "Vendor end" assessment meeting – 2 days.

2.4.3 Personnel Attending the Assessment Meetings

During the course of both the "user end" and "vendor end" assessment meetings, information was requested and/or questions were asked which could not be provided or answered by the personnel attending the meetings. In some cases it was possible to make contact with the required personnel and

to arrange for them to attend part of the meeting. In other cases this was not possible because the personnel were not available (or not at the office location where the meeting was being held).

For future assessments, the assessment project team should ensure that all the appropriate personnel attend at least part of the appropriate meetings. In practical terms it is likely that attendance at each of the assessment meetings will be arranged by the lead person being assessed at each end. This lead person should be made well aware of the topics that will be covered and be able to secure attendance of all the appropriate personnel.

2.4.4 Documentation Requirements

The NERC CIP standards, upon which the Cigré approach was based, is focused on achieving compliance through documentation which provides evidence of appropriate security. This poses some challenges for the use of NERC CIP for our purposes for a number of reasons:

- The documentation requirements are extensive, and the full suite of documentation is unlikely be under the control of one group;
- Unless the vendor/user is required to comply with the NERC CIP standards, it is unlikely that they will already have all the required documentation in place;
- Unless the vendor/user is familiar with NERC CIP, they are unlikely to fully understand the need for all the documentation;
- It is unlikely that that the vendor/user will have previously collated a full set of the required documentation.

The challenge of collating the required documentation became apparent during the "user end" assessment, as the user had not been informed that they should have as much of this documentation available as possible. We attempted to address this as part of the preparation for the "vendor end" assessment by sending a list of documentation requirements in advance of the assessment. This list is included as Appendix A. This was only partially successful, primarily because of a lack of appreciation that as much of the listed documentation as possible should be collated and ready for use during the assessment meeting.

For future assessments, the assessment project team should ensure that the required documentation list is issued in advance of the assessment, and the user/vendor is made aware that as much of this documentation as possible (i.e., that already exists) should be collated and made readily available for the assessment.

2.4.5 Reusability of "Vendor End" Assessment

One of the objectives of the work of the Cigré task force was to create an assessment process which would allow a vendor to satisfy a number of users that its external third party access arrangements are

secure, without the need for multiple assessments. In order to achieve this, a single "vendor end" assessment would have to be acceptable to a number of users.

However, the experience of having completed one "vendor end" assessment suggests that this may be achievable in generic terms, but is not readily achievable in specific terms, for the following reasons:

- The services provided by the vendor are dependant on the contractual agreement between the vendor and the user. Different contractual agreements may stipulate different security controls. Therefore it cannot be assumed that the results of the "vendor end" assessment are applicable to all users.

- Vendors provide services from different offices. For example, Siemens provides services for OPAL from its Oslo office. It will provide services for other specific systems from other offices. It cannot be assumed that the results of the "vendor end" assessment at one office are applicable to all of that vendor's offices.

- The technical architecture and platform used by the vendor to provide its services may differ according to the system being supported. For example, the OPAL services provided by Siemens utilise both a UNIX-based platform for the main system support, and a PC-based platform for the provision of services related to Electronic Data Interchange (EDI) messaging on OPAL. The PC-based platform has different security control requirements than the UNIX-based platform, but the PC-based platform may not be required for services to other users. Therefore, inclusion of the PC-based platform in the assessment may yield different results but may be unnecessary for some users.

3. Assessment Checklist

3.1 Introduction

This section of the document provides comments on the assessment checklist itself.

3.2 Comments

3.2.1 Relevance to "User End" and "Vendor End"

The draft Cigré checklist indicates the relevance of each checklist item to both the user and the vendor. During the kick-off meeting these relevance indications were discussed and a number were modified. In most cases, changes were made to indicate that particular checklist items were relevant to the vendor, where the Cigré version of the checklist had indicated that these items were not relevant to the vendor.

It should be noted that in some of these cases the changes were made simply to indicate that the items may be relevant to the vendor: this could not be confirmed until such times as the "vendor end" assessment was carried out.

This situation is likely to persist through further use of the checklist. It is not always possible to be prescriptive about whether or not a given checklist item will be relevant to the user, vendor or both in all circumstances. The relevance may differ from assessment to assessment, either due to the detailed contractual arrangements between the user and vendor regarding the services, or due to the technical architecture deployed for the external third-party connection (and the ownership of it or the responsibility for managing it).

For future assessments, the kick-off meeting should be used to discuss and agree the relevance of each checklist item to each party.

3.2.2 Structure of checklist

The draft Cigré checklist structure is taken directly from the NERC CIP standards, and is therefore broken down into the various NERC CIP sections as follows:

- Critical Cyber Asset Identification
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeter(s)
- Physical Security

- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

While this structure may be appropriate for NERC CIP, it did cause some practical problems during the course of the assessment, for example:

- Questions which all applied to the same personnel were not always grouped together in the same section, which meant that either these personnel had to remain present throughout the assessment meeting, or had to be called more than once to a part of the meeting. During the course of the assessment, the assessment project team attempted to group together appropriate questions as much as possible to try to minimise this problem.
- In some cases, questions in different sections cover similar topics and there was some confusion over whether topics had already been covered. The primary example of this was related to vulnerability assessments, which are covered in two different sections:
    - HH-005-1 - Electronic Security Perimeter(s)
      M4. Documentation of the Responsible Party's annual vulnerability assessment
    - HH-007-1 - Systems Security Management
      M8. Documentation and records of the Responsible Party's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s)

  The first section covers vulnerability assessment of access points to the Electronic Security Perimeter (ESP), whereas the second section covers vulnerability assessment inside the ESP.

As a suggestion for further work, the checklist could be re-designed to provide a more logical grouping of questions appropriate for the assessment process.

3.2.3 Content of checklist

The content of the checklist covers all aspects required by NERC CIP. There are potentially some aspects which are less important for external third party access assessment.

As a suggestion for further work, the checklist could be re-designed to provide a more specific set of questions appropriate for the assessment process.

4. Electronic Security Perimeter (ESP)

4.1 Introduction

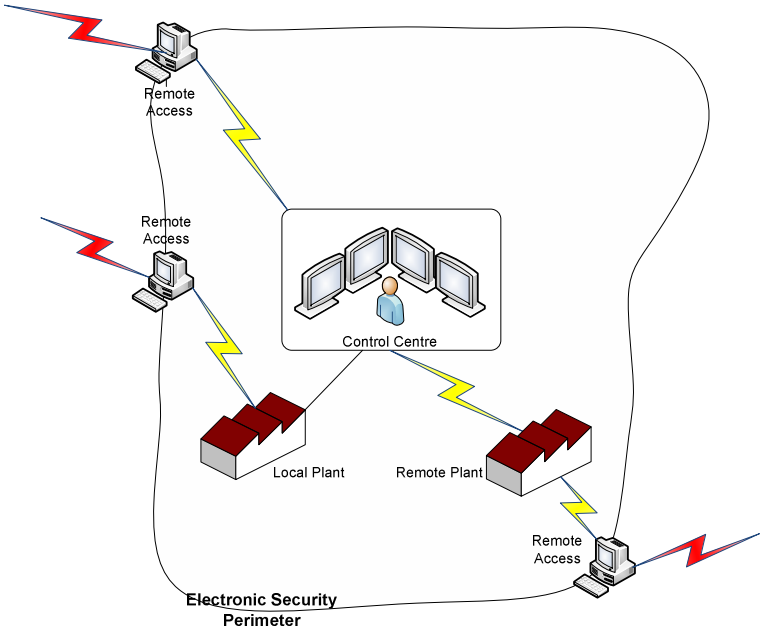
One of the key aspects of the NERC CIP based approach is the definition of ESPs. An ESP is essentially an electronic boundary around the systems being assessed. Any access through an ESP is via Access Points (APs), which should all be well known (documented) and secured.

The premise behind defining ESPs and APs is as follows:

- Everything inside an ESP is under your control;
- All the APs are under your control;
- You do not have any control over what is outside an ESP and may be trying to access it via any of the available APs (i.e., anything outside an ESP is untrusted).

4.2 Applying the ESP to External Third Party Access

For the purposes of the assessment, the statements above do not fully apply. Strictly speaking, the "vendor end" would be seen as untrusted by the "user end" and therefore outside the user's ESP. Likewise, the "user end" would be seen as untrusted by the "vendor end" and therefore outside the vendor's ESP. However, for the purposes of the assessment, the ESP must extend around both the "user end" and "vendor end" equipment which is necessary to facilitate external third party access. The ESP must be defined for both ends, and all APs through that ESP must also be defined. This is illustrated in the diagram below, where the APs are any connections to the remote access equipment (red connections in the diagram).



The degree of difficulty in determining the ESP and APs will largely be dependant on the level of networking present at each end (note that the example shown in the diagram above does not identify any APs to networking equipment such as routers, switches etc.). For example, if the vendor accesses the user's system from a single, standalone (i.e., non networked) workstation, with a dedicated communications link to the user's system (i.e., not via the vendor's corporate internet connection), then the ESP and APs are relatively easy to define. However, if the vendor accesses the user's system from multiple networked workstations, with a shared communications link to the user's system (i.e., via the vendor's corporate internet connection), then the ESP and APs are significantly more numerous and difficult to define. This will also present many more challenges during the assessment because there will be many more personnel involved in the definition of the ESP and APs, and controlling access using the APs.

Appendix A – Documentation Requirements List

All documents required have a document type associated with them. Document types are shown in the table below.

Document Type	Description
Policy	High level statements of goals and objectives and the general means of their attainment.
Program	A set of coordinated and related activities to meet a specific objective or set of objectives.
Plan	A set of coordinated and related activities which are triggered in response to specific events.
Process / technical document / procedure	Documentation of specific methods used, technical solutions deployed or steps taken to complete an activity.
List	Documentation identifying a number of similar "items" (e.g., personnel, assets).
Record	Documentation of a specific event having taken place.

The table below provides approximate quantities of each type of document required for complete coverage of all the stated requirements.

Quantity	Document type
1	Cyber Security Policy
2	Event triggered plans for Cyber Security Incidents and for Response and Recovery.
4	Lists of Critical assets, Critical cyber assets, Personnel authorizing access and Personnel having access.
5	Established programs for Information protection, Access control, Cyber security training, Personnel risk assessment and Patch management.
20 (approx.)	Recorded activities such as annual approvals of policy, plans and programs.
40 (approx.)	Documented procedures, processes or technical solutions.

The documentation requirements list is shown in the table overleaf.

Section Number	Section Topic			Document Type	Document Required
HH-002	Critical Cyber Asset Identification	M1	R1.1	Process / technical document / procedure	Documentation of risk-based assessment methodology to use to identify Critical Assets
		M2	R2	List	List of identified Critical Assets
		M3	R3	List	List of associated Critical Cyber Assets essential to the operation of the Critical Asset
		M4	R4	Record	Record of annual approval of list of critical assets and critical cyber assets
HH-003	Security Management Controls	M1	R1	Policy	Cyber Security Policy
		M1	R1.3	Record	Record of annual review and approval of policy
		M2	R2.1	List	Responsible manager
		M2	R2.2	Record	Record of changes of responsible manager
		M3	R3	Record	Exceptions to cyber security policy
		M3	R3.3	Record	Record of annual review and approval of exceptions
		M4	R4	Program	Information protection program
		M4	R4.3	Record	Record of annual assessment of information protection program
		M5	R5	Program	Documentation of access control program (for access to information)
		M5	R5.1	List	List of personnel responsible for authorizing physical or logical access to information
		M5	R5.1.2	Record	Record of annual verification of personnel responsible for authorizing physical or logical access to information
		M5	R5.3	Record	Record of annual assessment of processes for controlling access privileges to protected information
		M6	R6	Process / technical document / procedure	Change control and configuration management processes
HH-004	Personnel and Training	M1	R1	Program	Documentation of security awareness program
		M2	R2	Program	Documentation of cyber security training program
		M2	R2.3	Record	Record of training, including attendance records
		M3	R3	Program	Documentation of personnel risk assessment program
		M3	R3.2	Record	Records of application of personnel risk assessment to personnel

Section Number	Section Topic			Document Type	Document Required
		M3	R3.3	Record	Records of personnel risk assessment results
		M4	R4.1	List	List of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets
HH-005	Electronic Security Perimeter	M1	R1	Process / technical document / procedure	Documentation of Electronic Security Perimeter and all access points
		M1	R1.6	Process / technical document / procedure	Documentation of all interconnected cyber assets inside Electronic Security Perimeter
		M2	R2	Process / technical document / procedure	Documentation of access control procedures and technical mechanisms at access points
		M2	R2.2	Process / technical document / procedure	Documentation of ports and services configuration at all access points
		M2	R2.3	Process / technical document / procedure	Procedure for securing dial-up access (if dial-up available)
		M2	R2.4	Process / technical document / procedure	Authentication procedures for access through access points
		M2	R2.5.1	Process / technical document / procedure	Processes for access request and authorization
		M2	R2.5.3	Process / technical document / procedure	Review process for authorization rights
		M2	R2.6	Process / technical document / procedure	Documented content of appropriate use banner
		M3	R3	Process / technical document / procedure	Processes for monitoring/logging access at access points
		M3	R3.2	Record	Access logs
		M4	R4	Process / technical document / procedure	Access point vulnerability assessment process
		M4	R4.5	Record	Documentation of annual access point vulnerability assessment
HH-006	Physical Security	M1	R1.1	Process / technical document / procedure	Process for defining physical security perimeter
		M1	R1.2	Process / technical document / procedure	Processes to identify all access points through each physical security perimeter and measures to control entry at those access points

Section Number	Section Topic			Document Type	Document Required
		M1	R1.3	Process / technical document / procedure	Processes, tools, and procedures to monitor physical access to the perimeter(s).
		M1	R1.4	Process / technical document / procedure	Procedures for the appropriate use of physical access controls
		M1	R1.5	Process / technical document / procedure	Procedures for reviewing access authorization requests and revocation of access authorization
		M1	R1.6	Process / technical document / procedure	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
		M1	R1.7	Process / technical document / procedure	Plan update process
		M1	R1.9	Process / technical document / procedure	Annual review process
		M2	R2	Process / technical document / procedure	Controls to manage physical access (operational and procedural controls)
		M3	R3	Process / technical document / procedure	Controls to monitor physical access
		M4	R4	Process / technical document / procedure	Controls to log physical access
		M5	R5	Record	Logs of physical access
		M6	R6	Process / technical document / procedure	Documentation of maintenance and testing program
		M6	R6.2	Record	Test and maintenance records for physical security systems
		M6	R6.3	Record	Outage records for physical security systems
HH-007	Systems Security Management	M1	R1.1	Process / technical document / procedure	Cyber security test procedures
		M1	R1.3	Record	Cyber security test results
		M2	R2.1	Process / technical document / procedure	Process to ensure only required ports and services are open
		M2	R2.3	Record	Documentation of exceptions to requirement that only required ports and services are open

Section Number	Section Topic			Document Type	Document Required
		M3	R3	Program	Documentation of patch management program (may be part of change control and configuration management
		M3	R3.1	Process / technical document / procedure	Documented assessment of security patches
		M3	R3.2	Process / technical document / procedure	Documented application of security patches
		M3	R3.3	Process / technical document / procedure	Documented non-application of security patches
		M4	R4.1	Process / technical document / procedure	Documented implementation of AV/malware prevention tools
		M4	R4.2	Process / technical document / procedure	Documented non-implementation of AV/malware prevention tools
		M4	R4.2	Process / technical document / procedure	Documented process of signature updates
		M5	R5	Process / technical document / procedure	Documented controls for access authorization and accountability for all user activity
		M5	R5.1.2	Record	Logging (audit trail of account use)
		M6	R6	Process / technical document / procedure	Documented process and mechanisms for monitoring security events
		M6	R6.3	Record	Logs of security events
		M6	R6.5	Record	Record of review of security event logs
		M7	R7	Process / technical document / procedure	Procedures for cyber asset disposal/redeployment
		M7	R7.3	Record	Records of asset disposal/redeployment
		M8	R8.1	Process / technical document / procedure	Vulnerability assessment process for all cyber assets within the Electronic Security Perimeter
		M8	R8.4	Record	Documentation of annual vulnerability assessment all cyber assets within the Electronic Security Perimeter
		M9	R9	Record	Record of annual review of documentation and records of changes
HH-008	Incident Reporting and Response Planning	M1	R1	Plan	Cyber security incident response plan

Section Number	Section Topic			Document Type	Document Required
		M2	R2	Record	Cyber security incident records
HH-009	Recovery plans for critical cyber assets	M1	R1	Plan	Recovery plans