ES 2006-12-18

REPORT

External Third Party Access and Cyber Security

The Cigré taskforce on External Third Party Access and Cyber Security has completed its work in December 2006. The main result is delivered in form of an Excel file. A hyperlink is attached last in this status report.

Control systems have moved from analog to digital technology. Hardware alone is no longer defining the functionality. Identifying equipment and cabling on-site is no longer enough to identify control functions. Software upgrades are as important for the functionality. A few talented experts can also update installations all over the world given remote access. Future maintenance contracts are likely to include significantly quicker repair times if remote access is included. Use of standard operating systems, data manipulation and human interfaces lowers cost and facilitates upgrades. As the new digital technology minimizes the traditional mean time to repair it introduces a new risk of malicious destruction of functionality from viruses, worms and hackers. A new digital battlefield is established and cyber security becomes an important area to handle.

The general goal for this taskforce has been to facilitate the acceptance of remote access and build a common understanding among vendors and electric utilities on cyber security for remote third party access. Safe external third party access is a dual responsibility for vendors and utilities. As utilities are ultimately responsible for the electricity, it makes sense for them to review or audit the vendors given external access rights. Given the dual nature of the connection the first idea is obviously to audit each occurrence one by one. This idea however does not scale up to a large usage of remote access, as each vendor would be audit innumerable times from different utilities using different methodology.

The specific result of the work should be to establish a common platform for review or audit of the vendor side thus building trust and saving the work of multiple audits.

Active participants have been four major international vendors, four large utilities and two major consultants. As cyber security needs to reach far out in the field of control engineers we looked for a base standard that was openly available on the Internet. The methodology choice eventually centered on NERC CIP as being the latest most thorough attempt to-date to address cyber security issues. Each line in the resulting excel sheet thus corresponds to one NERC CIP requirement. However we apply those lines to all external third party access and do not restrict them to critical assets for the bulk electricity system that is the described target in CIP002. The phrase '*inspired by NERC CIP*' was thus coined to indicate that we are using the requirements and evaluations in NERC CIP but are not bound by the restrictions.

The first column in the excel sheet is called ‘*Dimension’*. It describes the requirements that are audited while the last three columns give room for more specific details in ‘*Suggested Audit Interpretation*’ in ‘*Scenario/Example*’ and in the specific ‘*CIP text*’. The column ‘*Relevance for 3rd party access*’ rules out a number of CIP requirements or limitations that are irrelevant to this task. *´Relevance to Utility Party’* is included to stimulate utilities to audit their end of the line also. The ‘*audit’* column is intended to be marked directly when the audit is done and the ‘*Level of compliance’* should be filled out later when the result have been analyzed probably by a separate group. Note that in some cases the rows have been split into two to cover evaluations that are more detailed than the original requirements. A number of advanced calculations were taken out at a late stage in order to keep this first version simple. The next step should be doing a table test type review or a review on a real system to check what the contribution of this work can be in real life.

In December 2006 the US Federal Energy Regulatory Commission Staff also issued its preliminary assessment of the NERC CIP standards. A sentence like ‘*The CIP Reliability Standards represent the most thorough attempt to-date to address cyber security issues for the Bulk-Power System*’ naturally strengthens the decision to use NERC CIP as base for this work. At the same time the assessment states that it ‘f*ocus largely on proper documentation …..regardless of the quality if its contents…*’. This of course raises the issue of what a review or audit using a standard can be expected to provide. It may well be that the experience and quality of the people doing the assignment is more important than the standard itself. Interpretation of results however is easier if different groups doing audits or reviews use the same model and documentation structure. The word audit also has a very specific legal context in some countries so we prefer using review/audit.

To summarize, the result of this taskforce should facilitate the acceptance of remote access and give a good structure to build reviews/audits on. The columns for ‘*Suggested Audit Interpretations*’ and ‘*Scenario/Example*’ are largely placeholders for growing experiences. We urge everyone using this template to send his or her experience to the chairman or secretary of this taskforce in order to build a larger knowledge base and best practices.

Erik Sandstrom
TF chairman

Attachments & Links:

Checklist; see =>

NERC CIP; see =>

TF members on next page

EXTERNAL 3rd PARTY ACCESS & CYBER SECURITY.

TF_AG.D2.02_04

ACTIVE MEMBERS			COMPANY		
NAME	E-MAIL	NAT.	COMP.	SERVICE	HOMEPAGE
Erik Sandstrom	erik.sandstrom@vattenfall.com	Sweden	Vattenfall	Utility	www.vattenfall.com
Andrei Vidrascu	andrei.vidrascu@rte-france.com	France	RTE	Transco	www.rte-france.com
Miquel Lopez	malopez@endesa.es	Spain	Endesa	Utility	www.endesa.es
Marc Tritschler	marc.tritschler@kema.com	UK	KEMA	Consult.	www.kema.com
Kjell R Gustafsson	kjell.r.gustafsson@se.abb.com	Sweden	ABB	Vendor	www.abb.com
Simon Almond	simon.almond@ps.ge.com	UK	GE	Vendor	www.gepower.com/networksolutions
Richard Link	richard.link@siemens.com	Germany	Siemens	Vendor	www.siemens.com
Ari Silfverberg	ari.silfverberg@fingrid.fi	Finland	Fingrid	Transco	www.fingrid.fi
Joe Weiss	joseph.weiss@us.kema.com	US	KEMA	Consult.	www.kema.com
Denis K Holstein	holsteindk@adelphia.net	US	OPUS	Publ.	www.opusss.com
Rodolfo Pellizzoni	rodolfo.pellizzoni@transx.com.ar	Argent.	Transba	Transco	www.transba.com.ar
Andres Cadenas	acadenas@ree.es	Spain	Red Elec.	Transco	www.ree.es
Luc Hossenlopp	luc.hossenlopp@areva.td.com	France	AREVA	Vendor	www.arevagroup.com