

WIB Mini Seminar

(19th of March 2008)

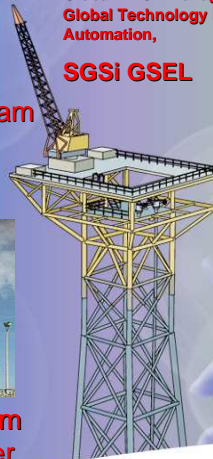


Ted Angevaare,
Global DACA Manager &
Global Technology Leader Process
Automation,
SGSi GSEL

Shell Upstream



Shell Downstream
and Gas & Power

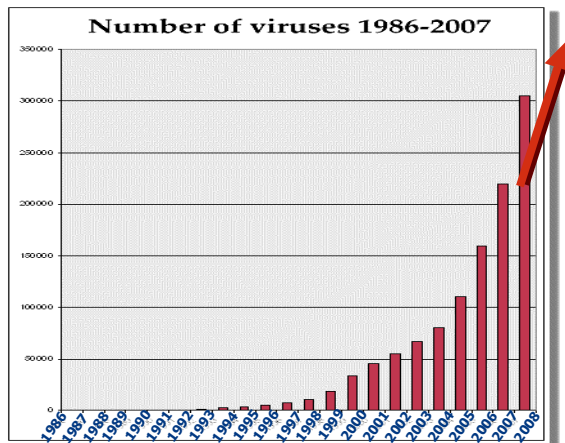


Why do we need Plant Security?

I don't want this!
We never had that
problem in the
past!



Asset Manager

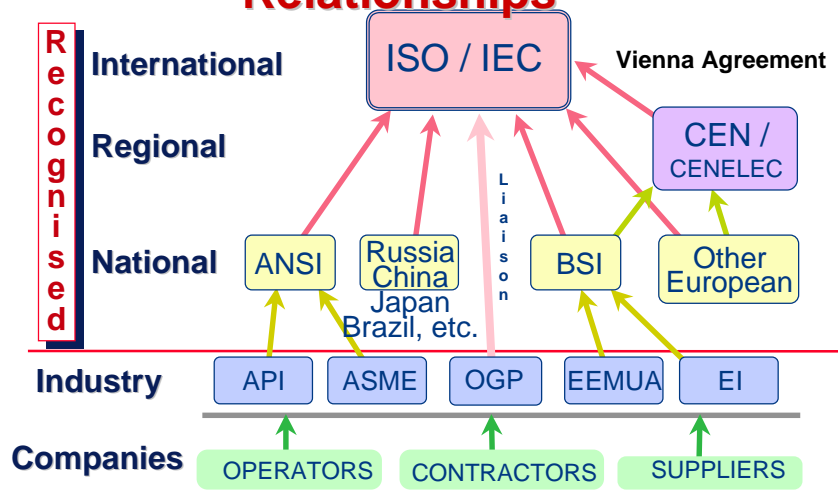


Today more than 300,000 computer viruses active worldwide!



Windows didn't bring only cheap software, but also many cyber security threats!

Standardization Bodies - Relationships



ISO developments in Information Security

ISO/IEC Work Group JTC 1 / SC27 (JTC1 Study Group on IT Security)

• **ISO/IEC 27000 family of standards:**

- ISO/IEC 27001 (2005) Specification for an Information Security Management System
- ISO/IEC 27002 (2005) Code of Practice for Information Security Management
- ISO/IEC 27003 ISMS implementation guidance (draft)
- ISO/IEC 27004 ISM metrics and measurements (final draft)
- ISO/IEC 27005 (2008) Information Security Risk Management
- ISO/IEC 27006 (2007) ISMS Requirements for bodies providing Audits and Certification
- ISO/IEC 27007 ISMS Guidelines for Auditing (draft)
- ISO/IEC 27008 Guidance on auditing information security controls (draft)
- ISO/IEC 27009 Information Security Governance (early draft, title uncertain)
- ISO/IEC 27010 ISM for inter-sector communications (draft)
- ISO/IEC 27011 ISM Guidelines for Telecommunications (awaiting publication)
- ISO/IEC 270... ..
- ISO/IEC 27032 Guidelines for Cyber Security
- ISO/IEC (new) Critical Infrastructure – Guidelines for CI providers (Telecom, Financial and the Energy sector)



ISO/IEC TR 27008

Ref: <http://www.iso27001security.com/html/iso27000.html>

International Certification



PCD Security

No international acceptable organisation available today:

- **Wurldtech – Achilles testing programme**
 - o Most DCS Vendors are obtaining this certificate already, e.g. ABB, Emerson, Yokogawa and Invensys Triconex) → **Ted Angevaare**
- **Mu Security – "MUSIC" Certification**
 - o Tested at our GSES Testlab Houston;
 - o The new MUSIC program consists of the Mu-4000 Security Analyzer appliance and its integrated engine and remediation documentation suite. → **Sean Kujawa**
- **CSSC (US-Cert Control Systems Security Centre)**
 - o The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.
- **ISCI**
 - o ISCI (ISA Security Compliance Institute), formerly CSSCO, facilitates the independent testing and certification of control system products against a defined set of control system security standards. Shell DACA is a full voting member. → **Marnix Haije**
- **Many more, however of lower quality....**



International Standards



PCD Security

Significant number of standards being developed:

- **AGA-12 (Cryptographic protection of SCADA Communications)**
- **API-1164 (Pipeline SCADA Security)**
- **Chemical Industry Data Exchange (CIDX) - Suite of standards**
- **IEEE P1686 – Substation IED Cyber Security Standard**
- **IEEE P1689 – Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access**
- **IEC 65C/WG10 (IEC 62443 (Security for industrial process measurement and control – Network and System Security) → **Herman Storey****
(Expected to be *the* industry security standard and based on SP99)
- **ISA-SP99 (4 volumes: ISA 99.00.01/02/03/04) → **Marnix Haije + Herman Storey****
- **NIST 800 - Series Security Guidelines**
- **CPNI (was NISCC - Produced a large number of Best-Practice papers) → **Ian Henderson****



Active members of the WIB Security Working Group

- Herman Suselbeek - WIB
- Tom Kuperij - WIB
- Frans Martens - Shell
- Maarten Oosterink - Shell
- Pascal van den Boogaard - Shell
- Lex Boekel - Wintershall
- Sierk Goedemoed - Heineken
- Marc Schuurman - Heineken
- Nate Kube - Wurdtech
- Ian Henderson - BP
- Annemarie Zielstra - NICC
- Auke Huistra - NICC
- Francis Boulu - Solvay
- Jos Menting - Laborelec
- Ted Angevaere - Shell (Chairman)



Ref.: <http://www.wib.nl/index.html>

Plan of Action:

The following subjects will be addressed:

1. Standards and Guidelines
 2. Certification
 3. Metrics
 4. Remote Access
 5. Security Management
- Assurance Process, e.g. Audits and Reviews

(Prevent overlap with other organisations/groups, such as:
LOGIIC, ISCI, SP99, etc.)



Ref.: <http://www.wib.nl/index.html>

Create Minimum Vendor requirements



PCD Security

1. Inventory of existing International Standards and Guidelines:
 - ✓ a. Use what has been completed by the PCSF: <https://www.pcsforum.org/groups/59/>
 - b. Google the internet for European Standards and Guidelines;
 - c. Use the Shell study as a basis to build on.

2. Investigation of standards used by Vendors:
 - a. Prepare clear questionnaire to the Vendor to investigate which Process Control Security standards are used by the Vendor.
 - b. Prepare list of main Vendors and contact persons (All)
 - ✓ c. Contact Vendors (Who: WIB) and explain what the intent is of WIB and what standards are used and/or which methodology.
 - d. Evaluate results from Vendors
 - Determine the applicable systems in Process Control Domains, its function and security objective. Create groups of subjects to be addressed as parts of Standards and Guidelines, such that all cyber security threats are dealt with.
 - ✓
 - Send information of step 1 and 3 on comment round to the members work group and collect comments. Evaluate comment and include modifications.
 - ✓
 - Create short list of International Standards, based on H, M, and L. Remove L from the list and produce new list.
 - ✓
 - Determine the detailed subjects of new standards that are still missing in the spreadsheet, e.g. ISO, IEC, BS, etc.
 - ✓

Ref.: <http://www.wib.nl/index.html>

Create Minimum Vendor requirements



PCD Security

- Investigation, evaluation and selection on the quality of the identified items of the Standards and Guidelines vs. the function and security objectives of the identified systems in the Process Control Domains.
✓ Approach is workshop 2 days Brussel at Laborelec, Linkebeek (near Brussels) on 21 and 22 Oct. 2008.
 - Create document with clear text from selected standards (SK). Review and improve document, i.e. 2 teams via teleconference. Decide on document lay-out and type of deliverable.
 - Start activity to have more WIB members in this workgroup or start the search for more WIB members because of this workgroup.
→
 - Send results from Linkebeek workshop to selected Vendors. Prepare information pack.
 - Invite selected Vendors to present their views on the subjects and to inform the WIB about their status of compliance.
 - Evaluate all Vendor's Feedback, make all the feedback information anonymous and publish the results to selected Vendors and to all WIB members in an anonymous manner.
12. Create a plan of action on the next steps....



Ref.: <http://www.wib.nl/index.html>

