SWEDISH EMERGENCY MANAGEMENT AGENCY

Information Sharing and Cooperation

Building Partnerships Between Private and Public Actors

SANS 2008 European Community SCADA and Process Control Summit, 8-11 September, Amsterdam

Dr. Åke J. Holmgren
Senior Analyst, Information Assurance Department, SEMA
Chair, E-SCSIE

SWEDISH EMERGENCY MANAGEMENT AGENCY

Background and Disclaimer

- SEMA has overall governmental responsibility for society's information assurance issues in Sweden
- SEMA has been working to increase the security of SCADA systems in critical societal functions for more than ten years
- SEMA supports this talk, but all comments and remarks does NOT necessarily represent the official position of SEMA
- This talk should NOT be viewed as the official position of the European SCADA and Control Systems Information Exchange (E-SCSIE)

SWEDISH EMERGENCY MANAGEMENT AGENCY

This Presentation

Take up where we left after Roger's (CPNI) talk…

- General comments on cooperation, information sharing, incident reporting, and vulnerability disclosure
- Vehicles for information sharing (a Swedish – international perspective)
- A few other European initiatives

SWEDISH EMERGENCY MANAGEMENT AGENCY

Cooperation

- Public-Private Partnerships is key
- Detailed technical regulations will not solve this!
- The ’culture clash on the plant floor’ continues all the way up through the government sphere
- Interdependent infrastructures and small nations calls for European and international collaboration
- Law enforcement must be more involved (SCADA forensics?)
- Cyber exercises are important, but industry must be involved in the planning and the feedback must be better

SWEDISH EMERGENCY MANAGEMENT AGENCY

Information Sharing

- Legal obstacles to information sharing (the 'FOI act', NDA, etc.)
- Cultural obstacles to information sharing ('turf war', commercial reasons, etc.)
- How far can we expand 'the circle of trust'?
- We need better processes for sanitizing information (protecting sources) and formal ways of sharing information
- Incident reporting and vulnerability disclosure are not the only types of information sharing!

SWEDISH EMERGENCY MANAGEMENT AGENCY

Incident Reporting

- National (homeland) security reasons as well as commercial matters makes it difficult
- Create an open format (template) for reporting incidents!
- Maintain closed industry data bases, but report general incident statistics openly

SWEDISH EMERGENCY MANAGEMENT AGENCY

Vulnerability Disclosure

- Structured vulnerability management is important
- How do we facilitate the distribution of vulnerabilities?
- The CERTs must reach out to the SCADA community, but can never be subject matter experts
- Not all vulnerabilities are created equal, but ranking is difficult

SWEDISH EMERGENCY MANAGEMENT AGENCY

Some facts about Swedish CIP/CIIP

- The concept of Total Defense (Societal Security)
- Previously, studies of 'local infrastructures' as part of civil defense planning
- Sweden has a long history of PPP
- CIIP and CIP are converging
- No list of infrastructures (The concept of Critical societal functions)

SWEDISH EMERGENCY MANAGEMENT AGENCY

Some facts about Swedish CIP/CIIP (Cont.)

Critical societal functions *comply* with one or both of the following conditions:

- A shutdown or severe disruption in the function, singlehandedly or in combination with other similar events, can rapidly lead to a serious emergency in society.

- The societal function is important or essential for responding to an existing serious emergency and minimizing the damage.

SWEDISH EMERGENCY MANAGEMENT AGENCY

Vehicles for SCADA Security Collaboration and Information Sharing

International	MPCSIE (The Meridian process)
EU	Euro-SCSIE
Bilateral	Various activities
National	FIDI-SC (Swedish industry) FIDI-SAMFI-SC (Swedish agencies)

SWEDISH EMERGENCY MANAGEMENT AGENCY

FIDI-SC

Members

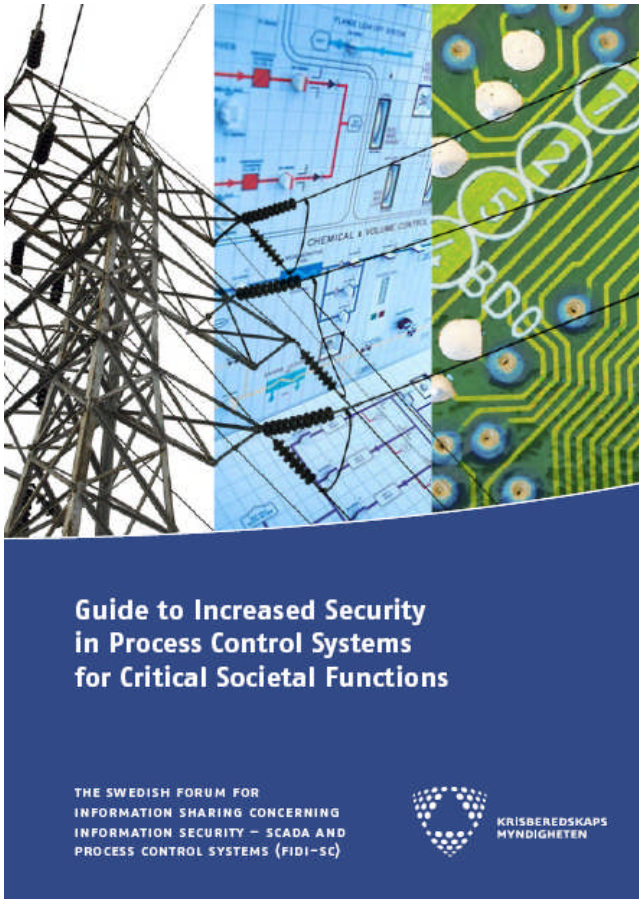
- Swedish National Grid (operator and sector agency)
- The railroad agency (operator and sector agency)
- 3 largest utilities (Vattenfall, Fortum, E.ON, > 80% of market)
- Largest oil refinery
- 2 largest water distribution/treatment companies (will include 2-3 more)
- Stockholm metro (the only one in Sweden)
- SEMA and Swedish Security Services

A few observations

- We cannot be threat-driven
- Government works as a facilitator, but must have technical knowledge to be a respected party
- It takes time and resources to build trust

SWEDISH EMERGENCY MANAGEMENT AGENCY

FIDI-SC SCADA Security Guide



Do we really need another guide?

Cross-sector guide in Swedish (English FYI)

Awareness-raising together with industry associations

Awareness-raising for CIO, CISO, CSO etc. (winter 2008/09)

Evaluation (revision) middle of 2009

SWEDISH EMERGENCY MANAGEMENT AGENCY

EuroSCSIE

"The European SCSIE (E-SCSIE) was formed 20 June 2005 and has held ten meetings. Its aim is for European industry, government, and research to benefit from the ability to collaborate on a range of common issues, and to focus effort and share resource where appropriate. The outcome would be a raised level of protection adopted across Europe's SCADA and Control Systems (SCADA/CS)."

"Ideally, each European country should be represented within the group with up to three representatives from government, industry (not consultancy or vendors) and research. Ideally the government and industry representatives should be sourced from a country's own SCADA Information Exchange, like e.g. Sweden's FIDI-SC. However, partial representation is acceptable."

SWEDISH EMERGENCY MANAGEMENT AGENCY

MPSCIE

The Meridian Process Control Security Information Exchange - MPCSIE brings together government officials worldwide who are policy-makers on issues of critical information infrastructure protection (CIIP).

The forum is open for government policy makers who are in the position to develop strategic and policy direction in protecting critical national infrastructure. Participation in the forum is open to all countries, with their government policy-makers participating in its activities.

SWEDISH EMERGENCY MANAGEMENT AGENCY

A Few Recent European Initiatives…

- The ESCoRTS project
- The WIB (International Instrument User's Association) European end-user group
- ERN-CIP – the EU pre-study of a European CIP lab network