Overview of the TG on IACS and Smart Grids

Testing Security: the critical infrastructure Operator's View
Workshop for Operators of Critical Infrastructures
September 12th 2013, Brussels

Annemarie Zielstra | TNO

Agenda

- TG on IACS and Smart Grids
- Our dream
- A Framework for IACS and Smart Grids
- Focus on People: Workforce Development Framework
- Focus on Technology: Future needs on testing

TG on IACS and Smart Grids: members

Asset owners, e.g.:

- **Shell**
- **E-On**
- **Laborelec/GDF Suez**
- **Alliander**
- **PSE Operator SA**
- **ENEL**
- **EDP**
- **PSE-operator**
- **Iberdrola**
- **TPEB**
- **Endesa**
- **Swiss Grid**

Vendors/Integrators/Consultancies:

- **Siemens**
- **ABB**
- **Honeywell**
- **Thales**
- **EOS**
- **Elster**
- **Infrastrutturecritiche**

Research/Academia:

- **TNO**
- **ENEA**
- **University of Gdansk**
- **GCSEC**
- **JRC**
- **Technical University Twente**
- **CERN**
- **Università CAMPUS BioMedico, Roma**
- **Universita' degli Studi di Napoli "Parthenope"**

Public Sector:

- **CPNI (UK)**
- **Cert-FI**
- **Govcert (DK)**
- **DEMA**
- **BSI**
- **MSB**
- **CNPIC**
- **ENISA**
- **European Commission**

3

Programme of work: starting points (1)

No overlap with existing initiatives

Close collaboration between DG's HOME, ENTER, ENER, CONNECT

TG on IACS and Smart Grids will fill in blind spots and will focus on the needs of the asset owners/end users

4

Programme of work: starting points (2)

Build on previous and existing initiatives, e.g.

- previous EU projects (ESCoRTS, ESTEC, …)
- ENISA, e.g Protecting Industrial Control Systems and Smart Grid Security
- EU Working Groups on Smart Grid Security
- …

Use network with other organisations

- EuroSCSIE
- EU-US Working Group on Cyber Crime and Cyber Security
- ICSJWG International Partners Day
- …

5

Our dream: A Resilient Digital Society in 2025

The key to a resilient digital society are critical infrastuctures that are safe, secure and resilient.

How do we get there?

By using an integral approach on People, Process and Technology.

IACS security is therefore an important topic for operators of critical infrastuctures, developers, manufacturers, system integrators and govern-ments.

6

Framework for IACS and Smart Grids Security

People	• Develop, test and certify the workforce that has interaction with IACS to make sure that they are cyber-aware, educated and trained • Create commitment up to and including the highest management level
Process	• Organisation, processes and procedures within asset owners and suppliers. • Already lot of existing initiatives / standardisation efforts (e.g. IEC/IAS 62443, ISO27019)
Technology	• Secure components and systems, being hardware as well as software

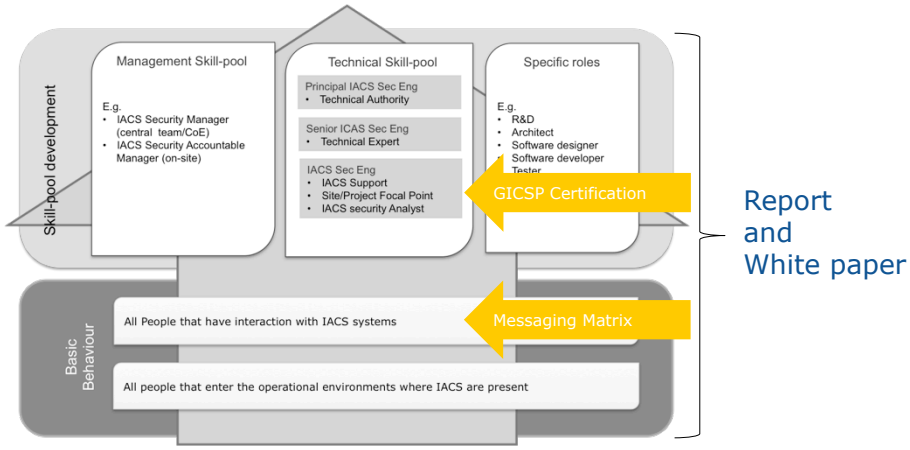
7

Status Tasks

People	•Draft Workforce Development Framework (incl Messaging Matrix) created, presented and discussed → Report + recommendations ready Q4 2013 •White paper WFD ready Q2 2014 •Industry Certification Global Industrial Cyber Security Professional (by GIAC) in development – planned Q4 2013
Process	•Out of Scope
Technology	•Preparation and distribution of a questionnaire seeking requirements from stakeholders for security testing (Q3-Q4 2013) •report on the results of the questionnaire (Q1-2014) •Based on the results of the questionnaire a more detailed time schedule for 2014 will be derived. This time schedule may contain the following milestones •report on methodology and standards for testing •report on test protocols •report on inventory of existing test centres for security testing for IACS & SG •report on gap analysis and final report

8

People: Workforce Development Framework



Technology: future needs on testing

What are the future needs on testing?

This Task will identify the main requirements for security testing of IACS by sending out and analysing the results of the questionnaire.

Asset owners have basically two important questions:

1. Are my systems safe and resilient against natural and cyber hazards?
2. How can I keep them safe and resilient in the future?

10

Neelie Kroes

"The more we rely on networks, the more we rely on them to be sucure. This calls for two things in particular.

First, our digital networks and systems are secure, resilient and trustworthy.

Second, we need our people to have digital skills.

Bringing these two together, I see a growing demand for cyber security skills. In the ICT sector in general, and for Industrial ICT in particular".

Conclusions

KEEPING OUR CRITICAL INFRASTRUCTURES CYBER RESILIENT IS A JOINT EFFORT.

Contact

Coordinator

Annemarie Zielstra
Director International Relations
Cyber Resilience | TNO
M +31 6 1299 2883
E annemarie.zielstra@tno.nl