



Control System Security and International Cooperation

- › Opening Control System Security Centre - Japan
May 27, 2013

***“Freedom means living with risk,
but without security,
risk means only threats,
not opportunities.”***

Lord Ralf Dahrendorf,
German-British sociologist, philosopher, political scientist and politician



TNO for Applied Scientific Research

The largest Dutch and one of Europe's leading independent Research and Technology Organisations (RTO):

- › Founded in 1932 by Dutch Government
- › Turnover 600 million EUR
- › Not-for-profit
- › Active in seven themes: Health Living, Industrial Innovation, Defence, Safety and Security, Energy, Mobility, Built Environment, Information Society
- › 4500 employees: 2100 university graduated (master level or PhD), 50 professor
- › Unique position between government and industry
- › Important role in the objectives of the Dutch government from terrorism, cyber risks and flooding
- › Provides research, development, engineering and consultancy services



TNO organisation for Applied Scientific Research

- › Assist in solving complex and challenging technical problems and technological innovations
- › Actively contribute to achieving the innovation goals stemming from our national Top Sectors Policy, the National Cyber Security Research Agenda and the European Union's Horizon 2020 programme
- › Involved in more than 55 security related projects in the 7th Framework Programme
- › Involved in the strategy development for the Netherlands on Cyber Security
- › Host of CPNI.NL from 2010-2012



Themes and innovation areas





TNO's mission

- › TNO connects people and knowledge to create innovations that boost the sustainable competitive strength of industry and well-being of society
 - › For industry and government; we work for a variety of customers
 - › Research is about the result; in everything we do, impact is the key

- › Cyber Security research is a key area of innovation needed to support our future:
 - › Working to solve the (cyber)security problems of our current and future infrastructure and systems
 - › Working with academe and industry to improve research tools
 - › Setting the R&D agenda for new topics with the most impact for our nation, including education



TNO | The Hague Security Delta (HSD)

- › TNO is one of the founding fathers of and an active partner in 'The Hague Security Delta' (HSD): the growing industry-government-research network in the security sector and champion of innovative security solutions and economic development in The Hague region. With revenues of 1.5 billion Euros and 10,000 jobs, the security sector is important to the Dutch economy
- › On behalf of HSD TNO is driving the Cyber Security and Urban Security 'innovation houses' forward by bringing the **Cyber Security Lab** and the **Cyber Incident Experience** into this cooperation
- › TNO is also the knowledge partner for the Serious Gaming, National Security, Dynamic Infrastructure and Forensics innovation houses, providing high-level expertise in technological and societal innovations as well as connecting them with and for a safer and more secure society



TNO | European and international collaboration

- › Close cooperation with the European Commission and ENISA
- › Chairman EuroSCSIE (European SCADA and Control Systems Information Exchange)
- › Coordinator ERNCIP (European Reference Network on Critical Infrastructure Protection) Thematic Group on IACS and Smart Grids
- › Chairman EARTO (European Association of Research and Technology Organisations)
- › Participating in EU-US initiative on Cyber Crime and Cyber Security
- › Collaboration with DHS Control Systems Security Programme
 - › the ICSJWG
 - › the ICSJWG International Partners Day
- › Collaboration with LOGIIC and DHS regarding the Workforce Development Framework
- › Collaboration with WIB Vendor Requirements (process of becoming an IEC standard)



TNO | European and international collaboration

- › Partnering with the World Economic Forum's initiative Risk and Responsibility in a Hyperconnected World
 - › Partnership for Cyber Resilience (PCR)
 - › Signing of the WEF principles



RTO's in the European Knowledge infrastructure

EARTO
(European Association of Research
and Technology Organisations)

350 RTO'S
chairman : Jan Mengelers TNO

Top 10 RTO's united in Europa:

- CEA
- Fraunhofer
- TNO
- VTT
- Sintef
- SP
- IMEC
- Tecnalía
- AIT
- DTI





Setting the agenda for: *'A more Resilient Digital Society'*

- › CRITIS 2013
September 16-18 2013, Amsterdam
www.critis2013.nl

- › Alert Online Campaign 'Smart Security'
October 28 – November 5 2013

- › High Level Dinner
November 4 2013, Amsterdam

- › The Grand Conference 2013 *Building a resilient Digital Society*
November 5 2013, Amsterdam
www.thegrandconference.org (by June 2013)



TNO and Process Control Security

‘Building a Resilient Digital Society’

- › Multidisciplinary approach
- › Technology – Humans – Process – Organisation - Governance
- › Experimental approach - evolve step-by-step into a mature solution
- › Strong expertise in and focus on domains:
 - › Defense
 - › Intelligence agencies and law enforcement
 - › Government: Security & Justice, Economic Affairs
 - › Critical infrastructures: Telecom sector, Energy sector, Service providers
 - › Cyber Security Technology Solution providers



It is all about

Protecting our (critical) assets:

1. Ensuring the safe, secure and reliable operation of manufacturing and production facilities



Preventing incidents that cause:

1. Unplanned disruption to project progress and/or
2. Product deferment or loss for manufacturing and production facilities
3. Cyber security related HSSE incidents



Cyber Security challenges in the PCD

Situation	<ul style="list-style-type: none">• Cyber security threats continue to increase in both frequency and sophistication• Process Control Systems are getting more automated, integrated and connected and are facing a real challenge• 'Learning by doing' (suffer incident and (hope to) do things better the next time) is dominant
Complications	<ul style="list-style-type: none">• To manage risk effectively in our industrial domains, technology standards, policies and practices are not enough, people are crucial• There is a lack of two fundamental underlying pieces to the puzzle: Awareness material about cyber security risks and consequences to inform both behavior and business decisions for operational resources Easily accessible, domain specific skill-pool and competency frameworks, training programs and materials A standardized foundational set of skills, knowledge and abilities for PCD IT Security across the industry is lacking, but useful <p>Technology is out there, but often human failures or bad implementation cause incidents</p>
Main question	<p>How do we ensure that our workforce in the industrial operations have enough Skills, Knowledge and Ability to keep the operational environment safe, secure and resilient against current and emerging cyber threats?</p>



Cyber Security challenges in the PCD

Answer

- **Behavioral change PCD Stakeholders:** Design, implement and operationalise an enterprise-wide PCD IT Security program to drive behavioral change at PCD stakeholders (boardroom, management, engineers, operators, contractors, vendors, integrators)
- **Skill-pool Management:** Design, implement and operationalise an enterprise-wide (ECO-system wide) PCD IT Security Skill-pool framework.



TNO Cyberlab

Learning by doing and Seeing is believing

- › Dedicated facility for Cyber Security Research project
 - › Technical infrastructure (hard- and software)
 - › Working space
 - › Demonstration space
 - › Awareness, education and training





Cyber Security Approach

Lines of development:

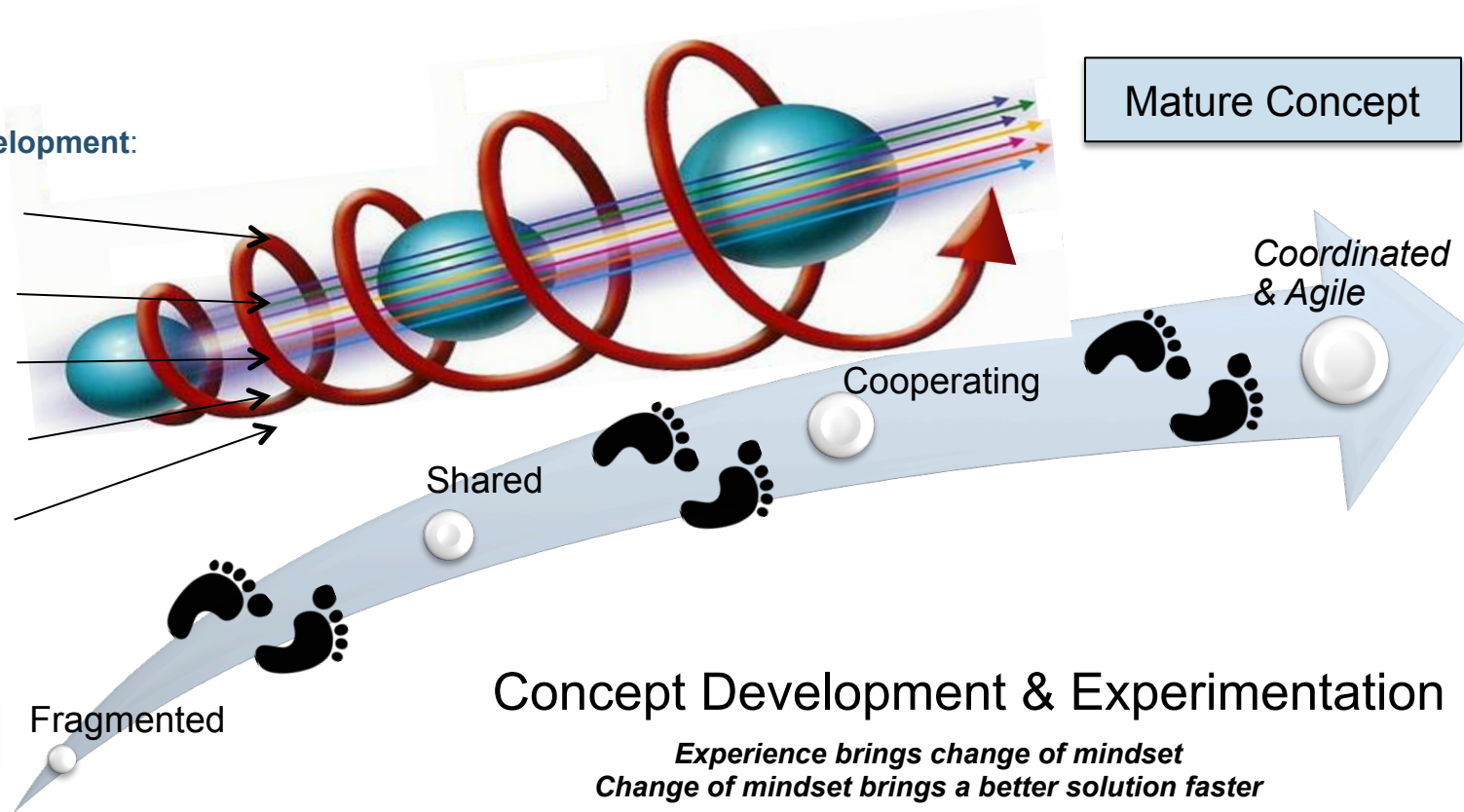
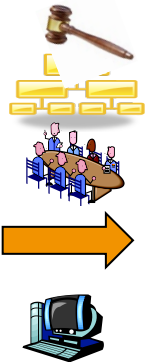
Governance

Organization

People

Processes

Technology





MOU between CSSC and TNO?

- › Hopefully we can explore opportunities for cooperation on the following topics:
 - › R&D on Industrial Control Systems / Shared Research Programme
 - › Technical expertise
 - › Situational awareness
 - › Training
 - › Monitoring and detection of networks
 - › Cyber Resilience
 - › Organising The Grand Conference Japan
 - › ...



Annemarie Zielstra
Director International Relations
Cyber Resilience
Chair EuroSCSIE
Coordinator ERNCIP TG
on IACS and Smart Grids

M +31 6 1299 2883

E annemarie.zielstra@tno.nl

