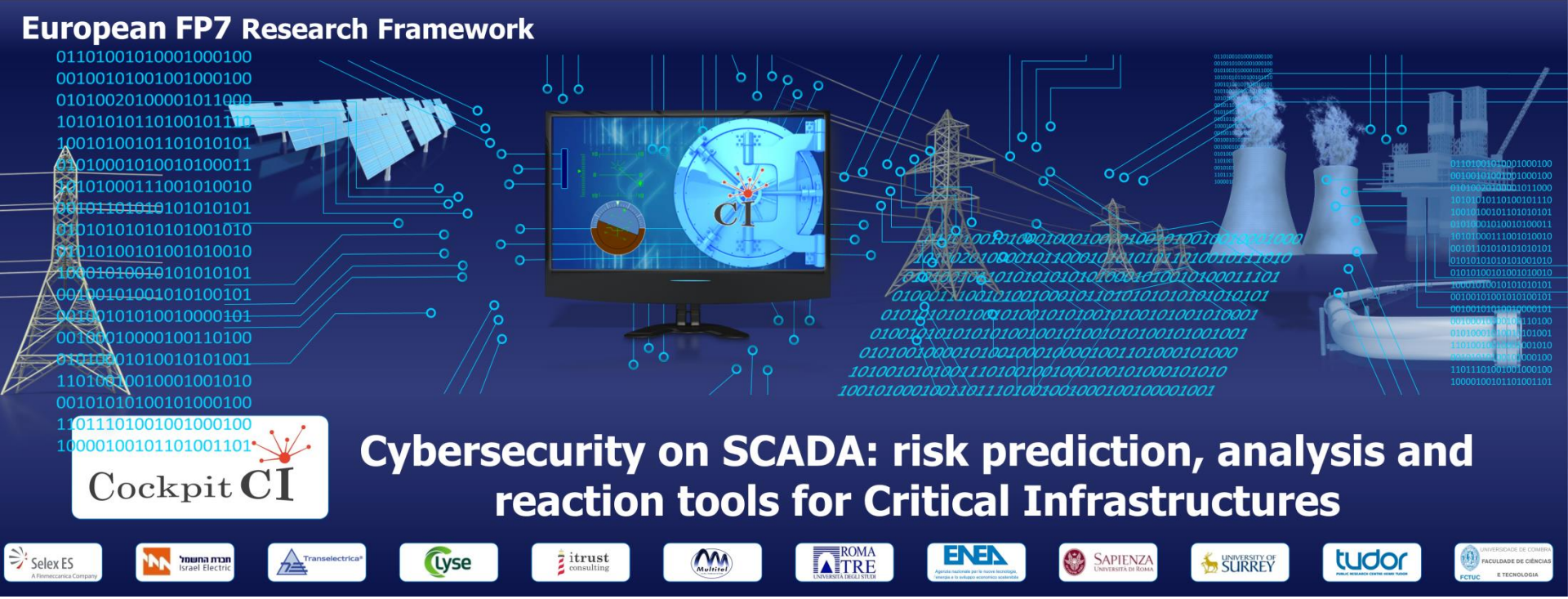


SCADA Cybersecurity Workshop 10th March 2014

Introduction

Dr. Carlo Harpes

itrust consulting

Information Society

Welcome to CREOS in Luxembourg

Welcome to CREOS in Luxembourg

Patronage by the Ministry of Economy Etienne Schneider

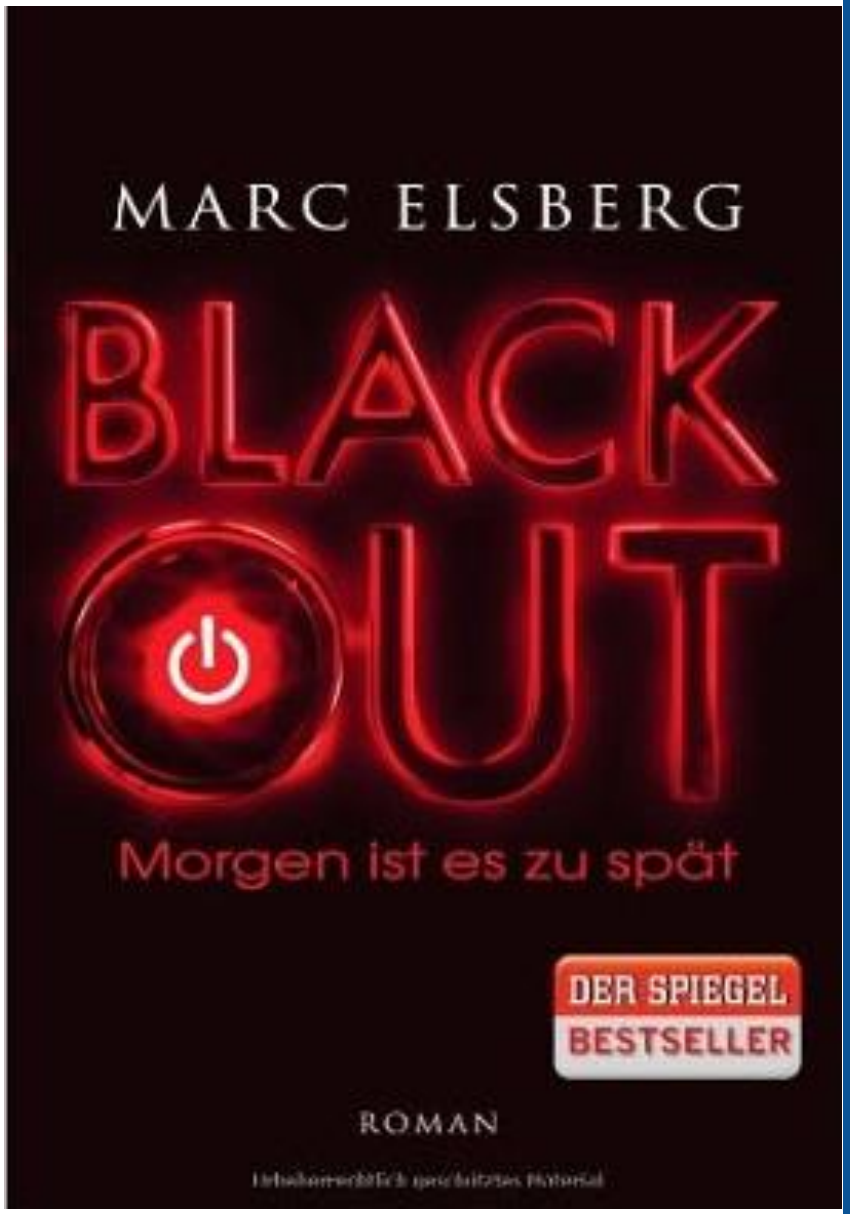
Thank you

Some motivation

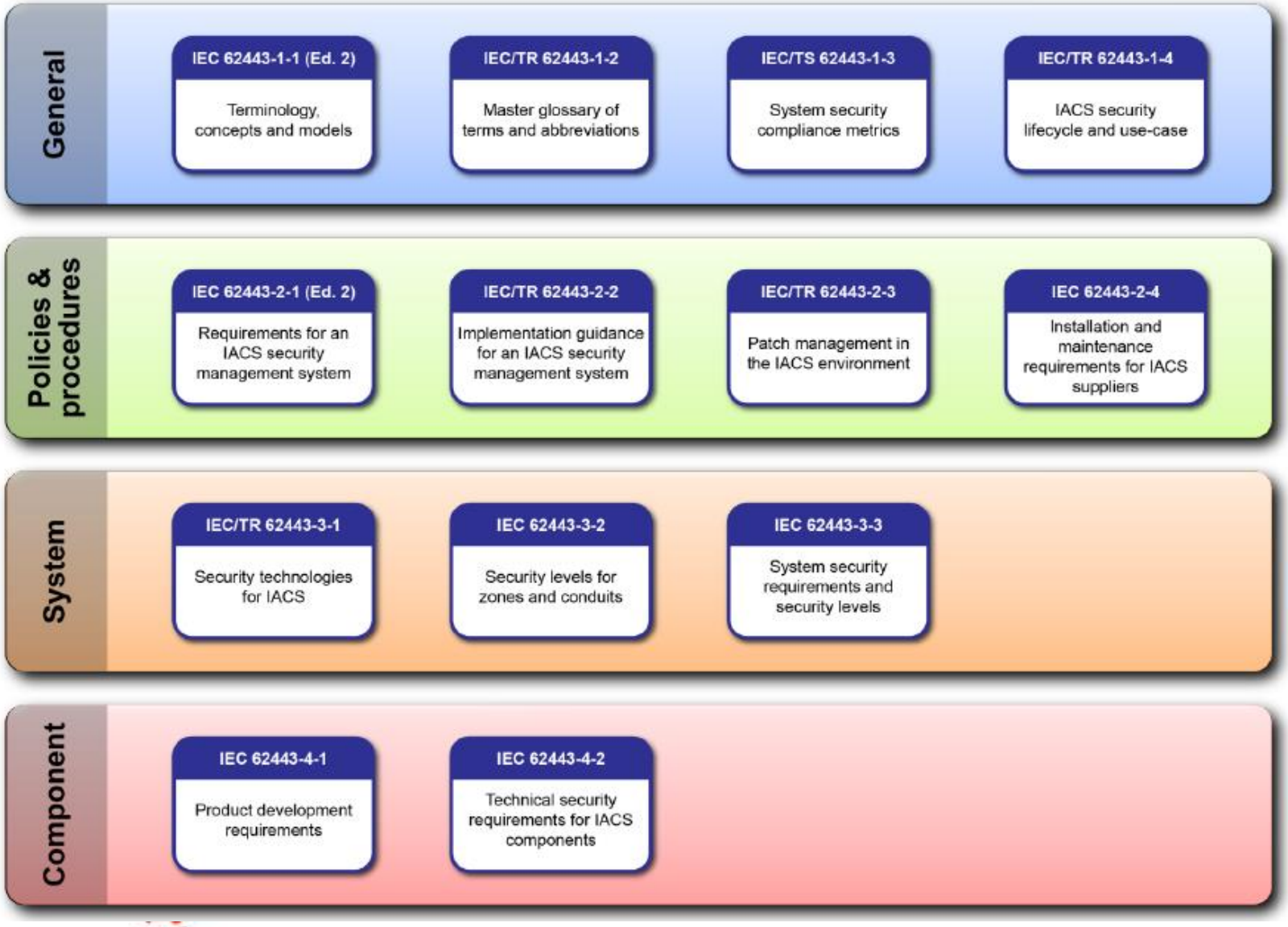
Bestseller related to Cybersecurity

http://
www.blackout-das-buch.de/
multimedia.html

http://www.youtube.com/watch?feature=player_embedded&v=uygGuJKiH5A



Standards – IEC 62443



Key topics

H2020-Objectives

DS-6-2014: Risk management and assurance models

Scope: The proposals should implement a pilot to demonstrate the **viability and scalability of state-of-the-art risk management frameworks**. The risk management framework will have to encompass methods to assess and **mitigate the risks in real time**. Work should include a **socio-economic assessment** to evaluate the **cost-benefit** of implementing the framework. The framework should be **dynamic, continuously adapted** to new ways of managing risk to keep up with the ever evolving threat and vulnerability landscape. New ways of dealing with the security risk resulting from **on-demand composition of services and massive interconnectivity** should be developed.

3rd CockpitCI Workshop

Objectives

A. **Present CockpitCI**
   Framework to allow the community of CI owners to detect, analyse and exchange real-time information about attacks in order to assess risk and avoid disastrous cascading effects,
   A few tools,

B. **Address security issues of operators**

C. **Get up-to-date on EU context**

A Workshop is sharing information, interactively !

Agenda

13:30	**Registration**	
14:00	Welcome to participants	Carlo Bartocci (CREOS) , François Thill (Ministery of Economy…, Carlo Harpes (itrust):
First Session		
14:15	Recent evolution of the CIP and CIIP for SCADA	Adrian Pauna (ENISA) via Skype
14:45	Experience of SCADA upgrading project	Carlo Bartocci (CREOS)
15:15	The Government as key stakeholder for CI Cybersecurity	Paul Rhein (Haut Commissariat à la Protection Nationale)
15:40	Overview of the CockpitCI Project	Antonio Graziano (Selex ES)
16:00	Coffee break	
Second Session		
16:20	The CockpitCI multi-layered detection framework	Paulo Simoes (FTUC):
16:35	Modelling SCADA and corporate network of a medium voltage power grid under cyber attacks	Michele Minichino (ENEA)
16:50	Risk Prediction Tool of CockpitCI system	Stefano Panzieri (Roma3):
17:05	Attributes extracted from network traces	Leandros Maglaras
17:15	Presentation of specific CockpitCI tools	Matthieu Aubigny (itrust)
Round Table		
17:30	Open discussion on security issues for SCADA operators and on CockpitCI's impacts.	moderated by C. Harpes (itrust)
18:00	Conclusion	C. Bartocci and C. Harpes
18:15	Cocktail	

Confidentiality – Trafic Light Protocol

We are a closed user group!

Amber for **CREOS presentation, discussions**

Green for **CockpitCI, tools, conclusions**

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED 	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER 	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN 	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE 	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

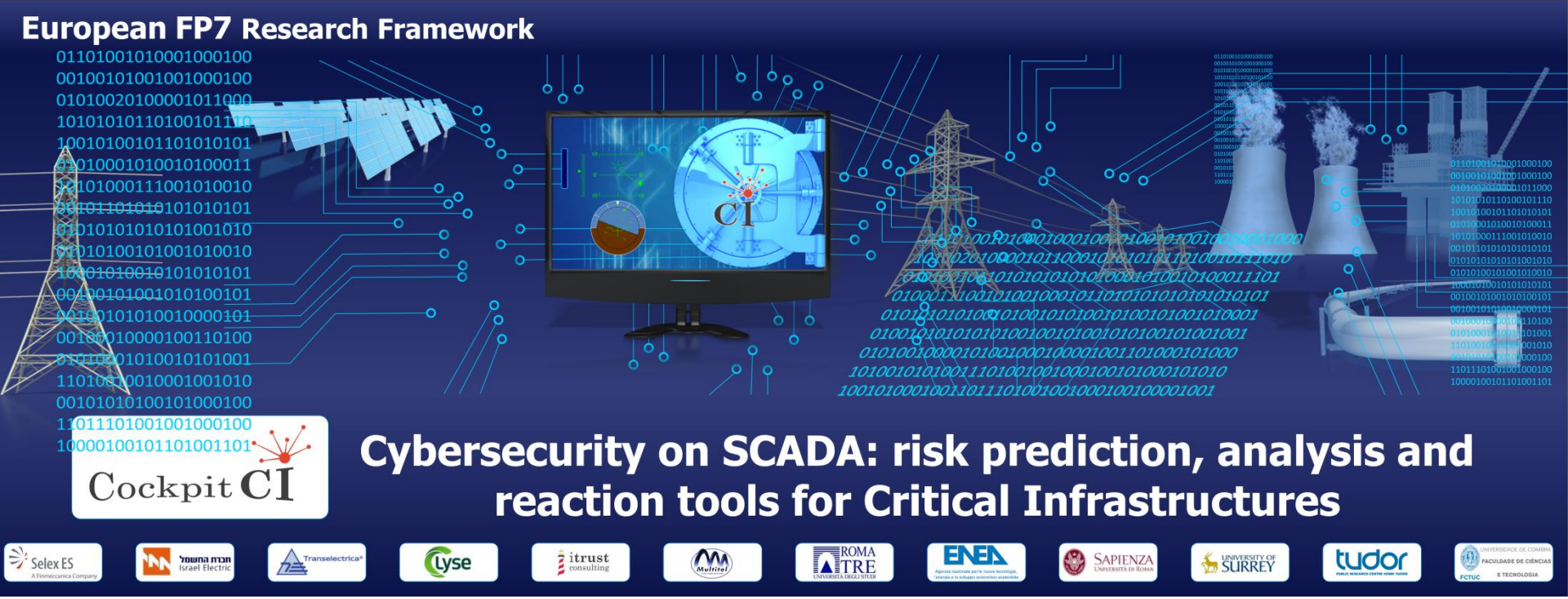
European FP7 Research Framework

Cockpit CI

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Selex ES · Israel Electric · Transelectrica · Lyse · itrust consulting · Multitel · Roma Tre · ENEA · Sapienza Università di Roma · University of Surrey · tudor · Faculdade de Ciências e Tecnologia

Any questions ?



Thank you for your attention