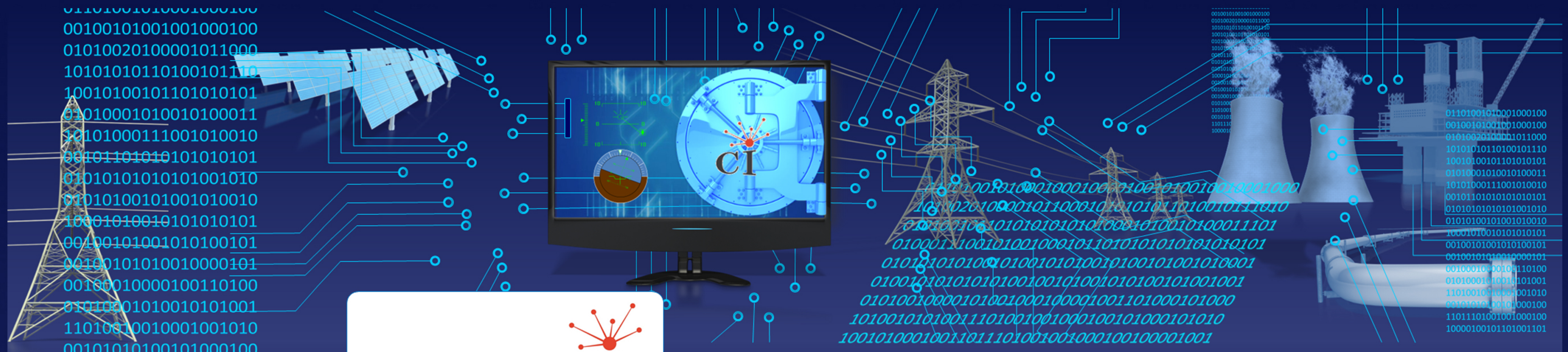


Cockpit CI

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

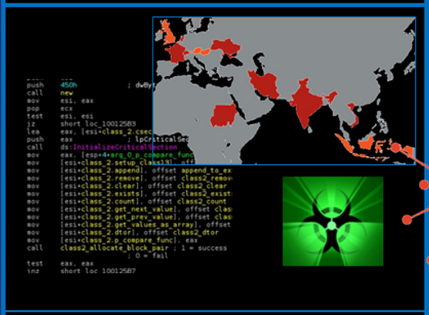
2012 2015

1965 US BLACKOUT

2007 AURORA experiment

2009 STUXNET

2011 DUQU



2013 RED OCTOBER

What next ?

Project Overview

Why a new research project?

1960s US blackout: industrial infrastructures are vulnerable.
1990s Italian electrical outage due to telecommunication failure shows that the interdependency of Critical Infrastructures is a serious problem.
Today, the emergence of sophisticated cyber-attacks shows that our technological societies are more vulnerable than we expected and ensuring security presents a new and primary societal challenge.

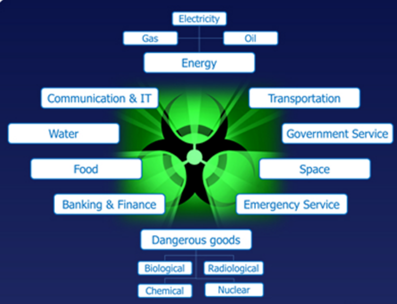
CockpitCI proposes to respond to this challenge by promoting a **global awareness approach** in order to:

- Keep infrastructures in operation safely in adverse situations;
- Maintain at least partial operational service rather than total shutdown.

CockpitCI aims to provide **a security and business support solution**, from a purely passive monitoring decision support tool (suited also for legacy systems) to a more sophisticated reactive solution.

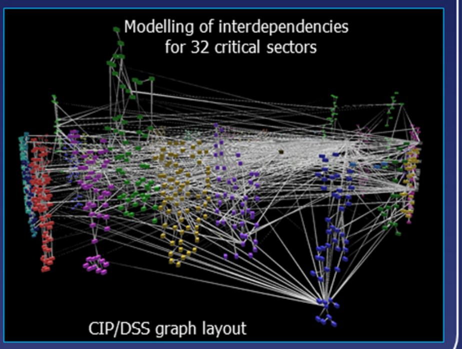
THE GRID MUST GO ON FOR EUROPE

European-PowerGrid by Shurita



Today, taking care of Critical Infrastructure operations and CI interdependencies is not sufficient

Stakeholders should consider the impact of Cyber Threat to avoid disastrous cascading effects and react before FATAL ERROR



Modelling of interdependencies for 32 critical sectors

CIP/DSS graph layout

Project Story

Follow-up of the previous FP7 MICIE project

Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures

The MICIE project has proved that predictive capability can improve the service level of interdependent CIs in uncertain situations caused by natural vulnerabilities.

NOT ENOUGH to quickly and effectively react to all adverse events, in particular to face cyber-attacks

The CockpitCI project aims to continue the research performed in the MICIE project and furthermore provide an effective solution to dealing with cyber-attacks on Industrial Control Systems (ICS) including its Control centre, communications networks and field equipment.

Promote a Global Awareness to Improve CI Resilience and Dependability

Cockpit CI

How?

- ▶ Automatic detection and analysis of cyber threats.
- ▶ Near real-time prediction of operational risk for Critical Infrastructures.
- ▶ Sharing of near real-time relevant info among CI owners to maintain QoS.
- ▶ Use of an IEC customised hybrid validation environment to test systems and strategies.

DETECT → ANALYSE → IDENTIFY → ASSESS → CLASSIFY → ALERT ON → SUPPORT → ACT

Cyber Attacks | QoS Impact | Operational Risks | Counter-Measures

Specifically: Identification of 6 innovative approaches to enforce SCADA awareness

☑ Integrated system
☑ Multi-layered Detection Framework
☑ Smart RTU
☑ Risk Predictor
☑ Risk Scenario Modelling
☑ Hybrid Validation Approach

www.cockpitci.eu

in CSACI^{2}P working group

European FP7 Research Framework