This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Workshop Introduction

Stefan Schauer

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

2nd HyRiM End User Workshop

Barcelona, 15.11.2016

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Workshop Goals

- Overview on current activities and results coming from the EU project HyRiM
- Presentation of novel approaches towards risk and security assessment for utility providers
  - Technical aspects (cyber-physical security, interconnected networks, threat propagation and cascading effects, surveillance, etc.)
  - Organizational aspects (risk management process, implementation of mitigation actions, etc.)
  - Societal aspects (multi-level resilience, influence of the human factor, effects on the supply chain, etc.)
- Presentation of real-life use case scenarios from different sectors (smart grids, water supply, oil refinement)
- Building awareness for these topics and for the project among potential end users

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Workshop Agenda
- HyRiM – Project Overview
- HyRiM – Project Ideas and Goals
- HyRiM – Project Results

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Workshop Agenda
- HyRiM – Project Overview
- HyRiM – Project Ideas and Goals
- HyRiM – Project Results

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Workshop Agenda

09:00 – 09:20	Welcome and Introduction to the HyRiM Project *Dr Stefan Schauer, AIT Austrian Institute of Technology (AT)*
09:20 – 10:20	A Multi-Level Approach to Resilience of Critical Infrastructures and Services *Dr Antonios Gouglidis, Lancaster University (UK)*
	The HyRiM Risk Management Process *Dr Stefan Schauer, AIT Austrian Institute of Technology*
	Analysing Operational Risks from Cyber-attacks in Future Smart Grids *Dr Paul Smith, AIT Austrian Institute of Technology (AT)*
10:20 – 10:40	Use Case: An APT Attack on Water Supply Systems *Karl Rossegger, Linz AG (AT)*
10:40 – 11:00	Short Break and Networking

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Workshop Agenda

HyRiM

11:00 – 11:50	Use Case: On Demand Surveillance Systems within an Oil Refinery *Massimiliano Turco, Akhela SRL (IT) and* *Gianfranco Porro, Sartec (IT)*
	Demo: Enhanced Surveillance Systems for Mobile ID Checking *Ali Alshawish, University of Passau (DE)* *Dr Stefan Schauer, AIT Austrian Institute of Technology (AT)*
11:50 – 12:40	Use Case: Ransomware Attack in a Smart Gird Environment *Alma Solar, Electrical Cooperative of Alginet (SP)*
	Demo: A Game-Theoretic Risk Assessment Tool *Dr Stefan Schauer, AIT Austrian Institute of Technology (AT)*
12:40 – 13:10	Demo: Estimating the Optimal Maintenance Strategy (HyRiM in Action) *Alberto Zambrano and Santiago Cáceres ETRA (SP)*
13:10 – 13:30	Closure of the Workshop

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Workshop Agenda
- HyRiM – Project Overview
- HyRiM – Project Ideas and Goals
- HyRiM – Project Results

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Key Points

- **Start of the project:** 01.04.2014
- **End of the project:** 31.03.2017
- **Project duration:** 36 Months

- **Project volume:** € 4,657,587.60
- **Funding:** € 3,387,085.00
- **Person months:** 440
- **Work program:** SEC-2013.2.5-4

- **Project Coordination:** AIT Austrian Institute of Technology GmbH
  Stefan Schauer (stefan.schauer@ait.ac.at)
  Christian Monyk (christian.monyk@ait.ac.at)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Partners

Name	Short	Country
AIT Austrian Institute of Technology GmbH	AIT	Austria
Universität Passau	UNI PASSAU	Germany
Lancaster University	ULANC	UK
ETRA Investigacion y Desarrollo SA	ETRA	Spain
Akhela SRL	AKH	Italy
Suministros Especiales Alginetenses COOP. V.	ECA	Spain
Linz AG für Energie, Telekommunikation, Verkehr und kommunale Dienste	LINZ	Austria

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

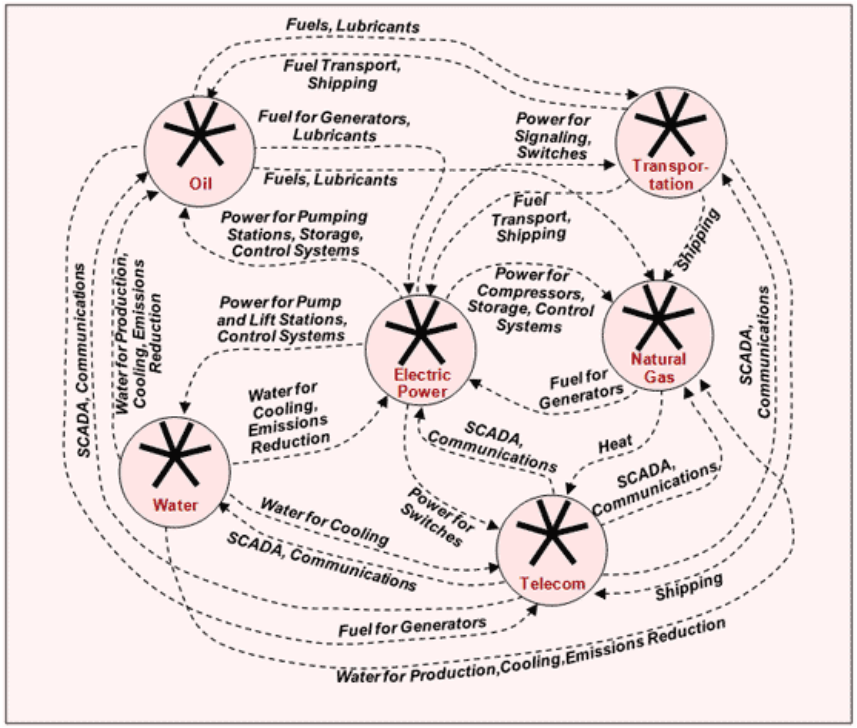
Contents

- Workshop Agenda
- HyRiM – Project Overview
- HyRiM – Project Ideas and Goals
- HyRiM – Project Results

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Idea

- Past few decades we experienced an increasing demand on utilities (water, electric power, oil, gas, transportation, etc.)
- Utility providers represent critical infrastructures which have to be secured
- Potential failures in utility networks (due to cyber-attacks or natural disasters) pose a major threat



Source: J. Peerenboom, R. Fisher, and R. Whitfield, 2001.

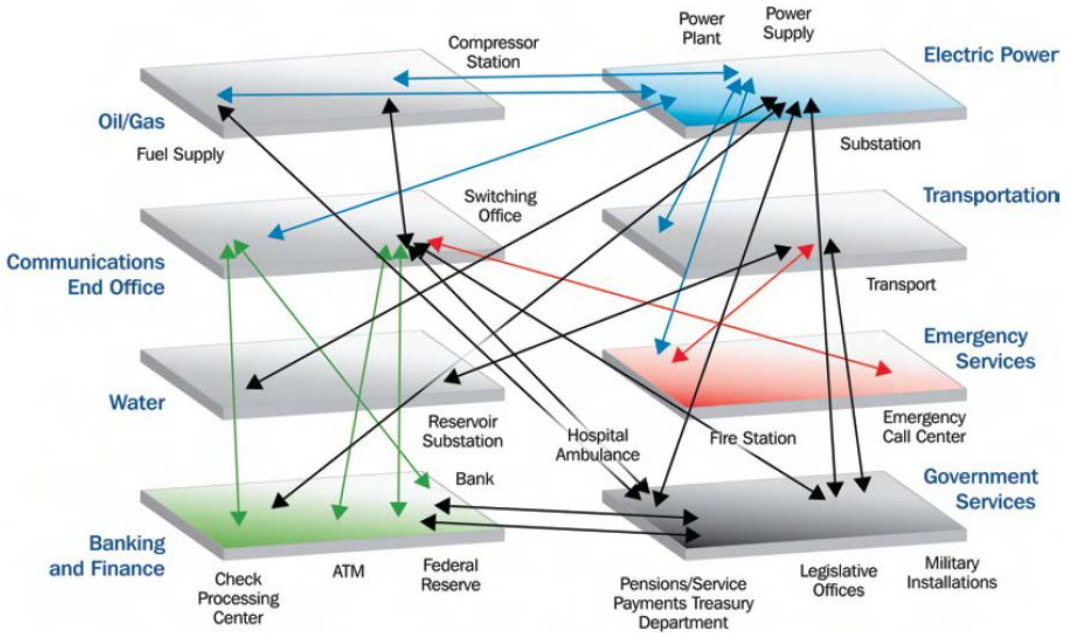
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Idea

- Interdependencies among various kinds of utility network infrastructures increase
  - Utilities and their control networks (e.g., SCADA systems) are interlinked with national and international partners
  - Bears new potential threats and attack scenarios

- Utility providers combine various networks within their infrastructures

- Attacks have cascading effects within a utility provider (e.g., between the control and utility network) or on other utilities

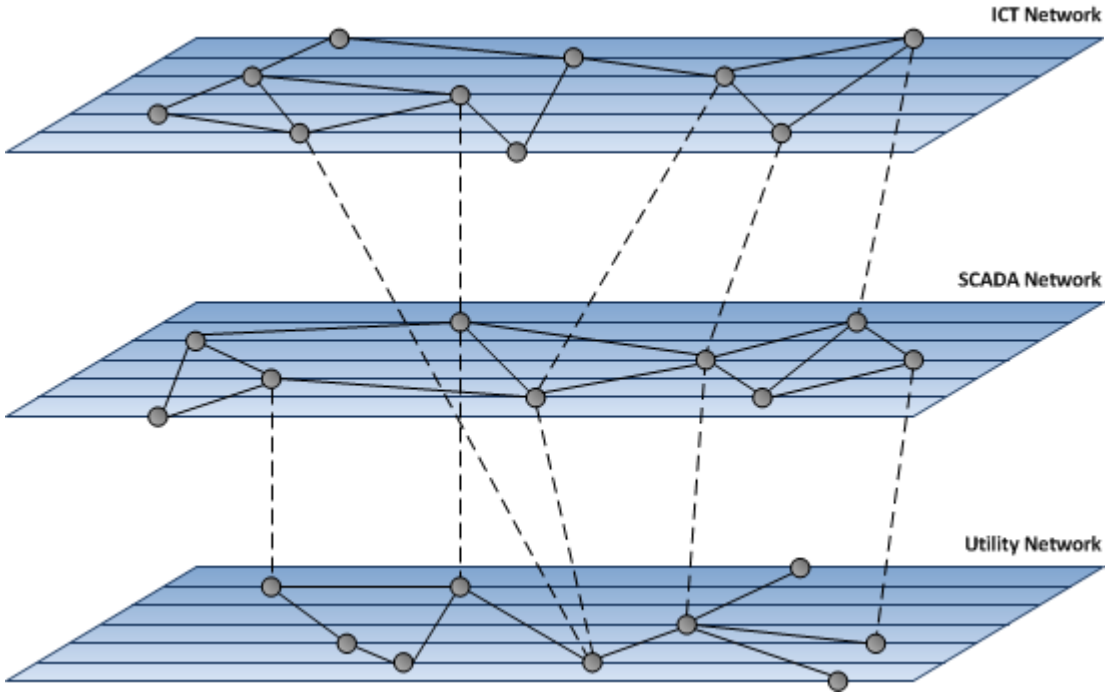


Source: Department of Homeland Security, National Infrastructure Protection Plan

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Idea

- Networks operated by utility providers are heavily connected among each other
  - Utility network (e.g. power lines, water pipes, oil pipelines, etc.)
  - Control networks (e.g. SCADA networks, smart grids, etc.)
  - ICT networks (e.g. office networks, communication networks, intranet, etc.)



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Project Idea

- HyRiM focuses on these interconnection points between control networks and individual utility networks, defining Hybrid Risk Metrics
  - Providing a quantitative (mathematical) approach to support decision makers
  - Assessing the potential threats and their cascading effects

- HyRiM focuses on organizational aspects and the human factor
  - Application of ethnographic studies to identify vulnerabilities arising from working conditions or social context
  - Evaluating and integration the effects of the human factor into risk metrics

- HyRiM focuses on novel surveillance technologies
  - Usage of personally owned devices (e.g., smartphones) to enhance surveillance technologies of the extended perimeter
  - Evaluating surveillance information to improve the Hybrid Risk Metrics

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Workshop Agenda
- HyRiM – Project Overview
- HyRiM – Project Ideas and Goals
- HyRiM – Project Results

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Results

- Definition of a mathematical framework for Hybrid Risk Metrics
  - Application of game theory and statistical methods
  - Considering unknown attacker behavior and decisions with unknown effects
  - Providing support for decision makers

- Consideration of organizational and human factors
  - Ethnographic studies within the pilot sites (Alginet, Cagliari, Linz)
  - Questionnaires and studies in cooperation with external organizations
  - Identification of critical aspects and potential vulnerabilities

- Assessment of current surveillance technologies
  - Threats detected and/or mitigated by surveillance technologies
  - Enhancement of surveillance using personally owned communication devices (e.g., smartphones)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Results

- Development of a conceptual approach to increase the resilience of critical infrastructures
  - Looking beyond pure risk management (i.e., preventive actions)
  - Measure to quickly recover if a malicious event has taken place

- Definition of the HyRiM Risk Management Process
  - Tailoring the ISO 31000 to the utility provider‘s world
  - Integration of existing HyRiM concepts and methodologies into the ISO 31000

- Formulation of use cases based on real-life scenarios
  - Malware/Ransomware spreading within a utility provider’s networks
  - APT attack on a utility provider’s control room
  - Physical intrusion into a utility provider’s premises

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Workshop Introduction

Stefan Schauer

stefan.schauer@ait.ac.at
AIT Austrian Institute of Technology
Lakeside B10a
9020 Klagenfurt
Austria

2nd HyRiM End User Workshop
Barcelona, 15.11.2016

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Project Objectives