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

An APT attack on Water Supply

LINZ AG, Lancaster University

Rossegger Karl

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.

Contents

- LINZ AG
- Questionnaire
- ATP Attack on water supply network

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

LINZ AG

LINZ AG

Austrian Infrastruktur Service Provider
2600 Employees

LINZ AG STROM

Energy
Telecommunications
Energy-Services

LINZ AG MANAGEMENTSERVICE

Finance, Legal

LINZ AG SERVICE

Water, Disposal

LINZ AG LINIEN

Public Transport

LINZ AG GAS/WÄRME

Gas, Heating

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

Questionnaire

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

Questionnaire

- **Security standards**
- **Risks**
- **Hardware, software**
- **Data protection and security**
- **Security checks**
- **Security issues**
- **Technical control devices**
- **Communication network**

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

Questionnaire - Outcomes

- **Positive understanding, workplace and private**
- **Security issues are largely detected**
- **A high degree of trust in the company**
- **A low perception of one‘s personal contribution**
- **Employees with certification are more sensitized**
- **Less transparency in the incident process**
- **Technical control devices have a great potential**

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

Data Flow Management

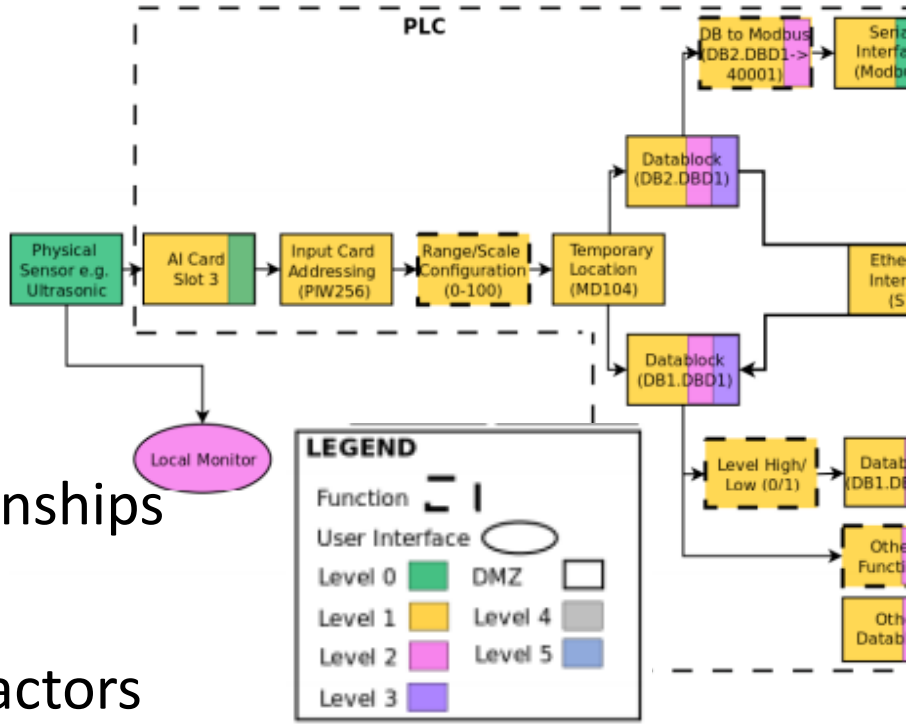
- **Estimate where all the risks lie**

- The process includes:
  - Identify physical processes
  - Identify people responsible
  - Perform (high level) vulnerability assessment

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

Outcomes

- Prepare data flow maps
- Improve our understanding
  - Technical data flows
  - Processing points
  - System-to-system relationships
- Investigate human (social) factors
  - System-to-user relationships



Data flow example of a single sensor*

* B. Green, M. Krotofil, and D. Hutchison, "Achieving ICS Resilience and Security through Granular Data Flow Management", Proceedings of the Second ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC 2016, Vienna, Austria, 28 October, 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

APT Attack - Overview

Setting up game theoretic model for cyber attack on water supply system

- Define goals to be optimized
- List of threats (attack strategies)
- List of countermeasures (defence strategies)
- Estimate payoffs for each scenario

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

APT Attack - Goals

- **Maximize availability**
- **Minimize cost**
- **Minimize damage of reputation**

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

APT Attack - Threats

- **Attack RTU (Man in the middle attack)**
- **Change program logic in a PLC**
- **Get physical access to a building**
- **Eavesdrop communication**
- **Insert malicious code on a SCADA server**

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

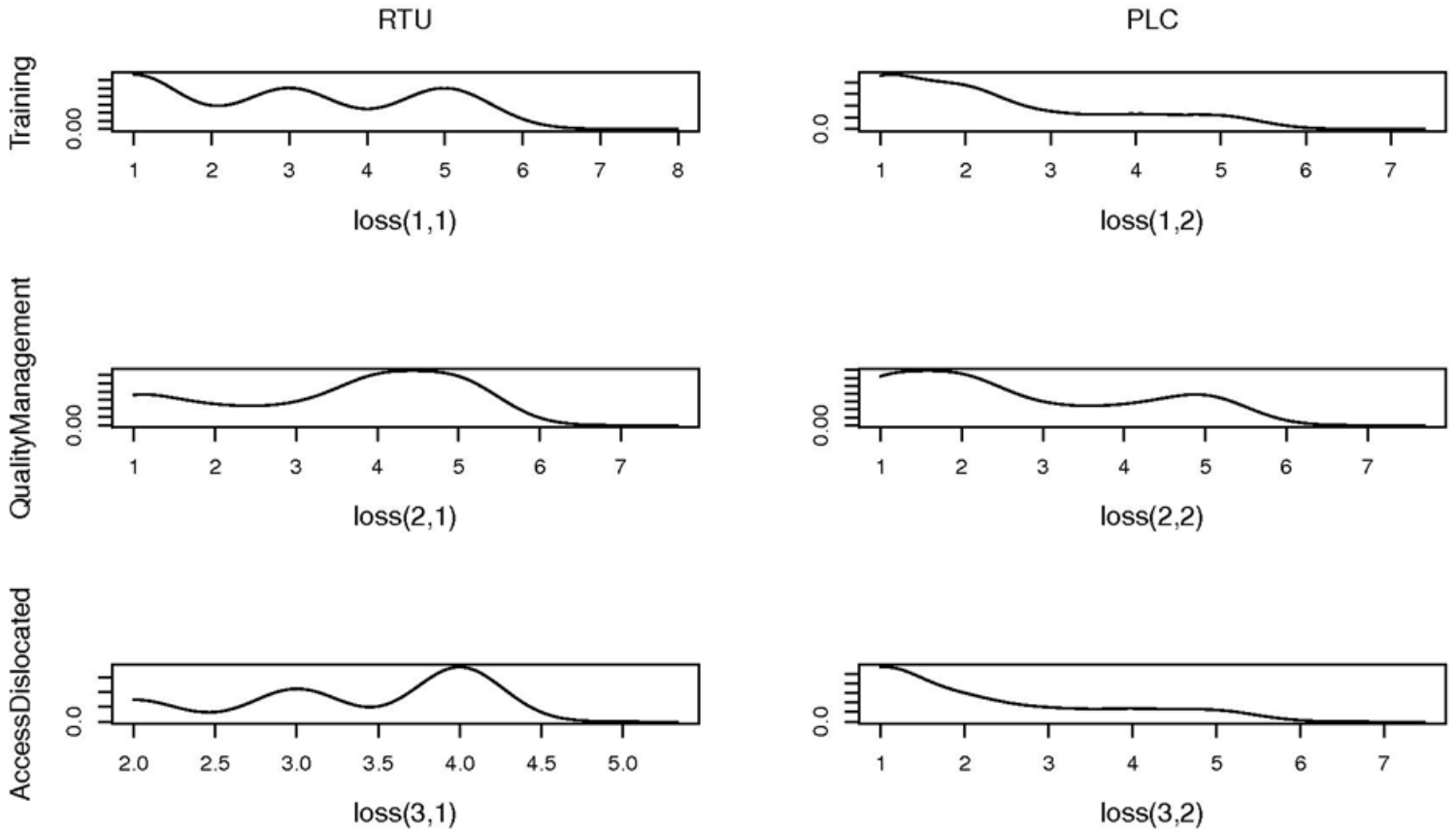
APT Attack - Countermeasures

HyRiM

- **Train awareness of employees (training)**
- **Increase quality management (corrective and preventive actions)**
- **Increase physical security of dislocated places**
- **Change physical access policy**
- **Secure administration of switches**
- **Check integrity of configuration more frequently**

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

APT Attack - Estimate Payoff Distribution



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

Contacts

- **LINZ AG**
  - **Rossegger, Karl, k.rossegger@linzag.at**
- **Lancaster Universtiy**
  - **Gouglidis, Antonios a.gouglidis@lancaster.ac.uk**
- **Austrian Institute of Technology**
  - **König, Sandra, sandra.koenig@ait.ac.at**