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

Risk Management for APTs
A Water Utility Case Study

Antonios Gouglidis

Novel Approaches in Risk and Security Management for Critical Infrastructures

Vienna, 19th and 20th September 2017

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

- Case study description
- Application of the HyRiM process
  - Establish the context
  - Risk identification
  - Risk analysis
  - Risk treatment
- Concluding remarks

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

Case study description

HyRiM

- European water utility organisation
- Provide its services to more that a hundred municipalities in its region
- Responsible for planning, building and maintenance of the whole network -- focus on the water quality
- The management, storage and delivery of water is supported by an ICS

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

Assume the threat of an APT

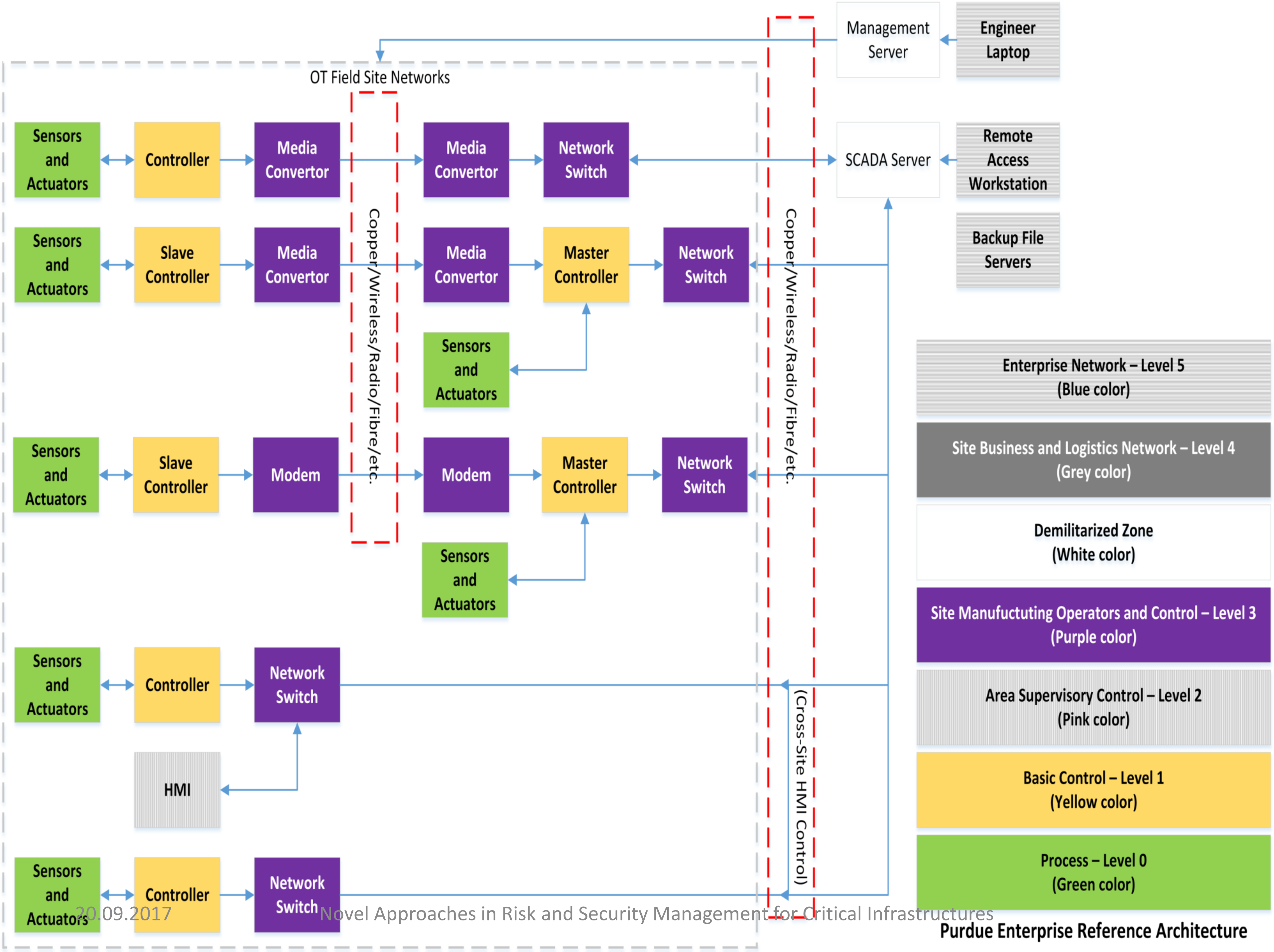
- Collect information using Open-source Intelligence (OSINT)
- Deploy spear phishing attacks to individuals
- Try to visit the facilities or contact external contractors for alternative entry points
- Review collected information for potential attacks

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

Establish the context

- Define objectives that should be achieved; understand internal/external factors that may influence the goals

- Main goals
  - Minimise the damage caused by an attack to the provided service
  - Minimise monetary damage caused by the attack (e.g. technical or legal nature)
  - Minimize reputation damage
- Multi-level analysis: Purdue enterprise reference architecture, social review analysis, business process analysis



Enterprise Network – Level 5
(Blue color)

Site Business and Logistics Network – Level 4
(Grey color)

Demilitarized Zone
(White color)

Site Manufucting Operators and Control – Level 3
(Purple color)

Area Supervisory Control – Level 2
(Pink color)

Basic Control – Level 1
(Yellow color)

Process – Level 0
(Green color)

Purdue Enterprise Reference Architecture

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

Risk identification

- Understand a range of scenarios describing what could happen, how and why
- Threats on main assets
  - Radio jamming/data manipulation
  - Becoming a HMI/master
  - Backup servers
  - Target external resources
  - …
- Identify potential vulnerabilities

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

Vulnerability identification*

- ClearSCADA server: CVE-2014-5411, CVE-2014-5412, CVE-2014-5413
- Network switches: CVE-2001-0895, CVE-2014-5412
- Controllers: Siemens SIMATIC S7-300 , S7-1200, ET 200S PLC, …
- Management server: SIMATIC STEP 7, Connecter Components Workbench, TIA Portal, ...

* Vulnerabilities as identified in Lancaster's emulated ICS testbed

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

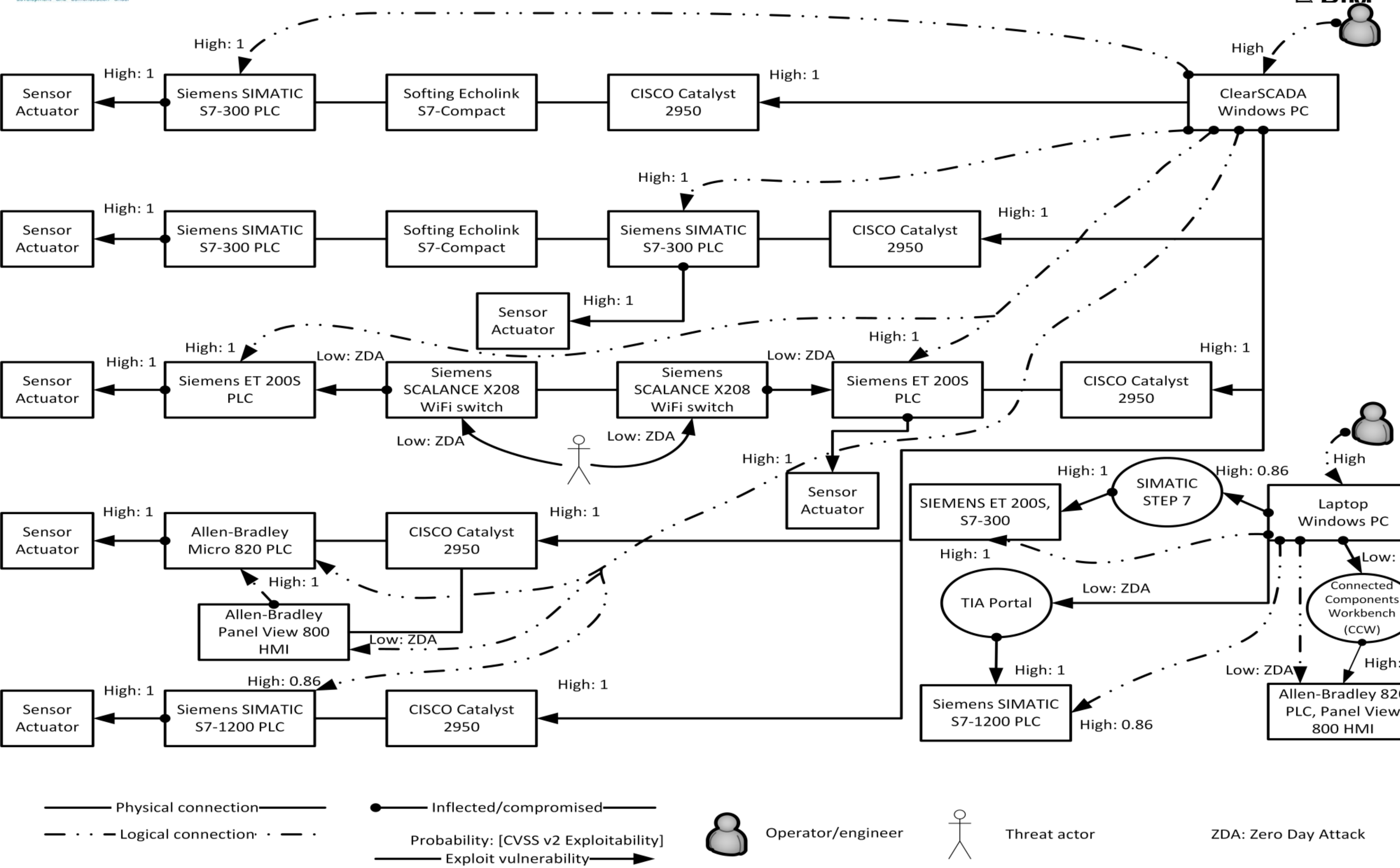
Risk analysis

- Develop an understanding of each risk, its consequence and the likelihood of these consequences

- Investigate the likelihood of events
  - Vulnerability assessment (CVSS)
    - Exploitability metric

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under

Estimation of likelihood via CVSS



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

Risk treatment

- Identify optimal set of controls to reduce the maximum damage that can be caused by an attacker to a minimum

- Define attack strategies/vector – 4 main categories
  - Operator -> ClearSCADA/Windows PC -> Cisco Catalyst
  - Operator -> ClearSCADA/Windows PC -> Siemens SIMATIC S7-300 PLC -> Sensor/Actuator
  - Engineer/contractor -> Laptop/Windows PC -> SIMATIC STEP 7 -> SIEMENS ET 200S PLC -> Sensor/Actuator
  - Threat actor -> Siemens SCALANCE X208 -> Siemens SIMATIC ET 200S PLC -> Sensor/Actuator

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

Defence strategies and frequency

- **Do not change anything**
- **Training**: Annually, per 2 years, new personnel
- **Password change**: Annually, when device is changed, when people are changed
- **Update**: automatic, annually, major updates
- **Patch/replace**: upon failure to operate, annually, major vulnerabilities
- **Manual checking of water**: Daily, weekly, monthly

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

Damage estimation

- Collect experts opinion for each scenario defined of a defence strategy and an attack strategy

- Damage is assessed by experts on a 5-tier scale
  - Very low, low, medium, high, very high

- 4 experts were asked to estimate the damage for each of the goals

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

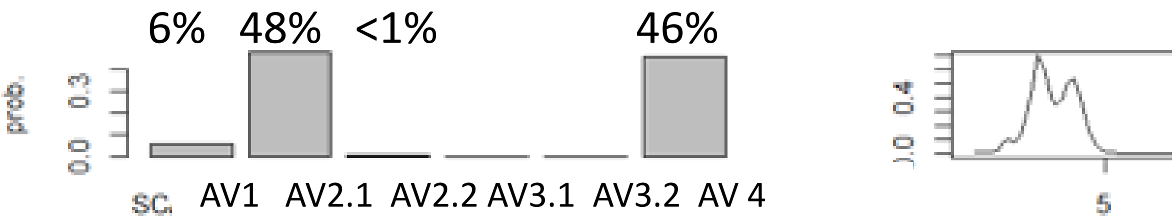
Game-theoretic optimisation

- Set up a game to find the optimal defence strategy and worst-case damage
- Computation of equilibrium (`R` package `HyRiM`)

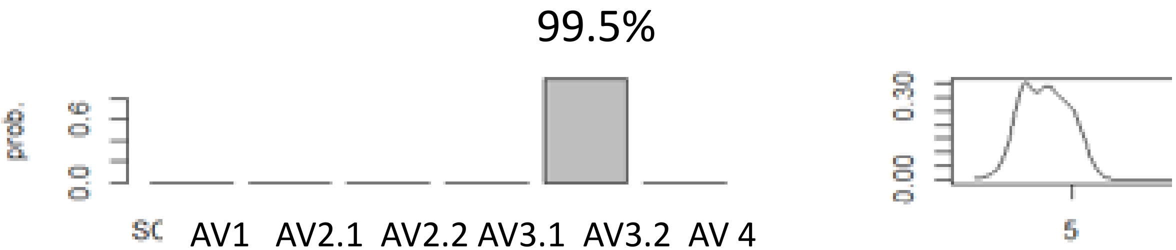
	Train annually	Train new personnel	Apply major updates	Patch devices upon failure	Patch major vulnerabilities
Frequency	2.8%	0.1%	88.3%	0.2%	8.6%

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

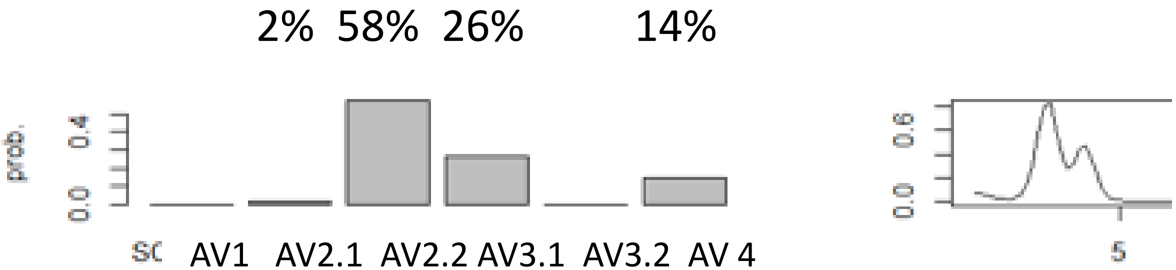
Worst case damage



worst case for goal 'Service'



worst case for goal 'Cost'



worst case for goal '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.

Concluding remarks

- The HyRiM process resulted in defining an optimal protection strategy in the treat of an APT
  - Improve security posture of the organisation
- Based on the collected data
  - Many defence strategies do not contribute in reducing the damage (only 5 out of 16 does)
- The frequency of the selected 5 strategies was determined and worst-case damage has been estimated per goal

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

Thank you!