11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Cyber Targets Water Management

Pieter Burghouwt[a], Marinus Maris[a], Sjaak van Peski[a], Eric Luiijf[b],
Imelda van de Voorde[b] and Marcel Spruit[a]

[a] *The Hague University of Applied Sciences*
[b] *Netherlands Organisation for Applied Scientific Research TNO*

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

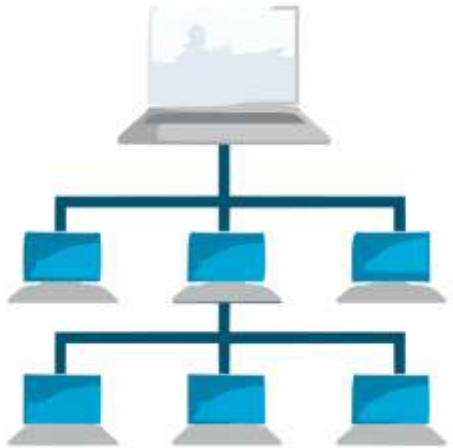
TNO innovation for life

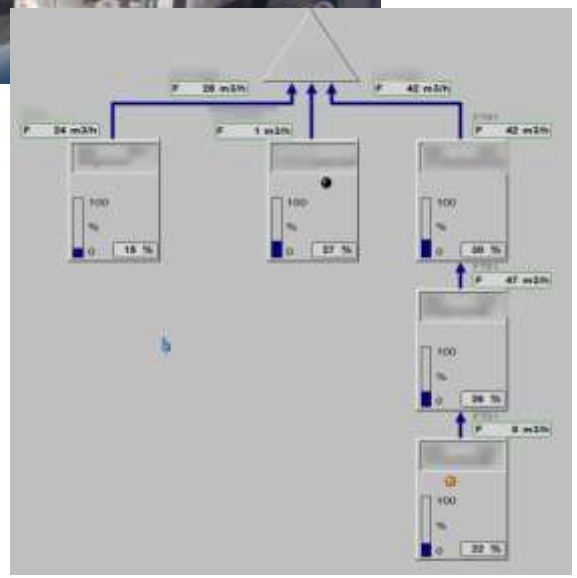
Outline

1. Introduction to Water Management in The Netherlands
2. The Cyber Security Benchmark
3. Observed ICS-related security dilemmas
4. The Cyber Security Simulator
5. Conclusions & Future work

1. Introduction to Water Management in The Netherlands from the past

1. Introduction to Water Management in The Netherlands: the present





Bron: waterschappen.nl

2. The Cyber Security Benchmark

- Objective: determination of the current state of ICS security in the water management sector

- Questionnaire with 48 open and closed questions
- Simple and fast
- Update of a benchmark questionnaire that was used for the drinking water and electricity sectors[1]
- Results allow for anonymous comparisons (confidentiality controlled by the Traffic Light Protocol[2])

1. *Luiijf, E., Ali, M., Zielstra, A.: Assessing and improving scada security in the dutch drinking water sector. International Journal of Critical Infrastructure Protection 4(3), 124–134 (2011)*
2. *CIP: Traffic light protocol (tlp). https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Traffic_Light_Protocol_%28TLP%29 (2015), visited April 2016*

2. The Cyber Security Benchmark

48 Questions cover five areas:

- 9 x Security Organisation
- 8 x ICS Deployment
- 8 x ICS Telecommunication
- 7 x ICS Personnel
- 16 x General

out
rec

New or improved questions on:

- Outsourcing
- IPv6
- Personnel screening
- Pen-testing
- Monitoring & Reporting of security incidents
- Physical security measures
- ICS security topics that need to be addressed

2. The Cyber Security Benchmark

Results (*19 water management organisations participated*):

- Significant differences between the participants in protection
- Examples of problems observed *in some organisations*:
  - limited management awareness for ICS-related risk
  - no or limited separation between office network and ICS network
  - limited security controls on outsourcing of ICS installation and operation
  - limited cyber attack monitoring capabilities
  - default manufacturer passwords or group passwords in certain situations (often because of legacy)
  - security patching is far from being performed according to the base-line requirement

3. Observed ICS-related security dilemmas

CRITIS 2016

1. **Patching vs. Continuity**
   Software updates prevent exploitation of known software vulnerabilities
   … but can cause process disruption
2. **Isolated vs. Centralised control**
   Internet technology and COTS solutions allow for simple central control
   … but can result in undesired connectivity between compartments and/or the Internet
3. **Automation vs. Disaster Recovery Capacity**
   Automation allows for staff reduction
   … but can result in a longer solution time in case of a major disaster that involves multiple sites

4. The Cyber Security Simulator

Objectives:

- **Create awareness**
  Demonstration of attack scenarios raises awareness of cyber attacks, the related threats, and the consequences in process control systems
- **Increase knowledge**
  Executing various cyber attacks and related (technical) controls on a realistic but scaled platform increases practical knowledge about vulnerabilities and controls

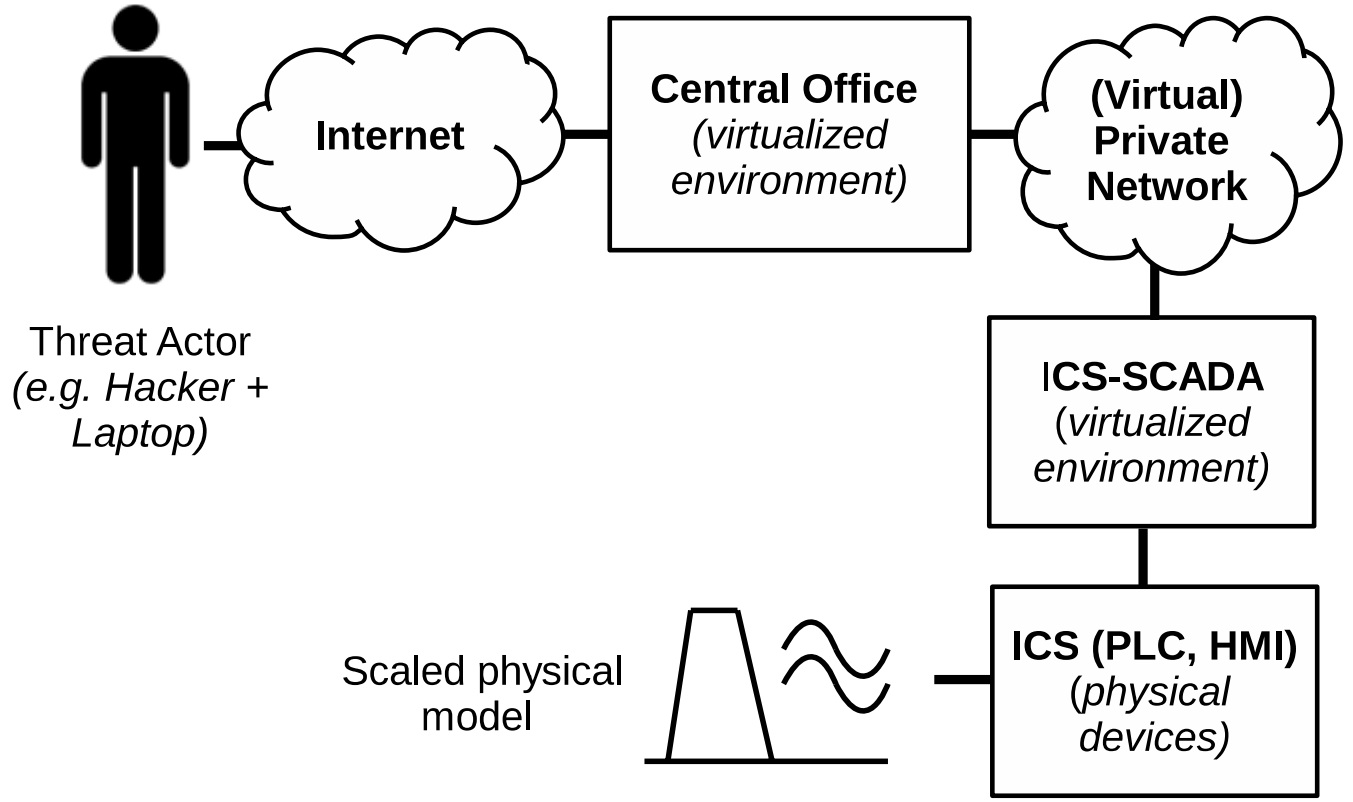
Additional requirements:

- Flexible and modular design
- Realistic configuration
- Clear insight in cyber attacks

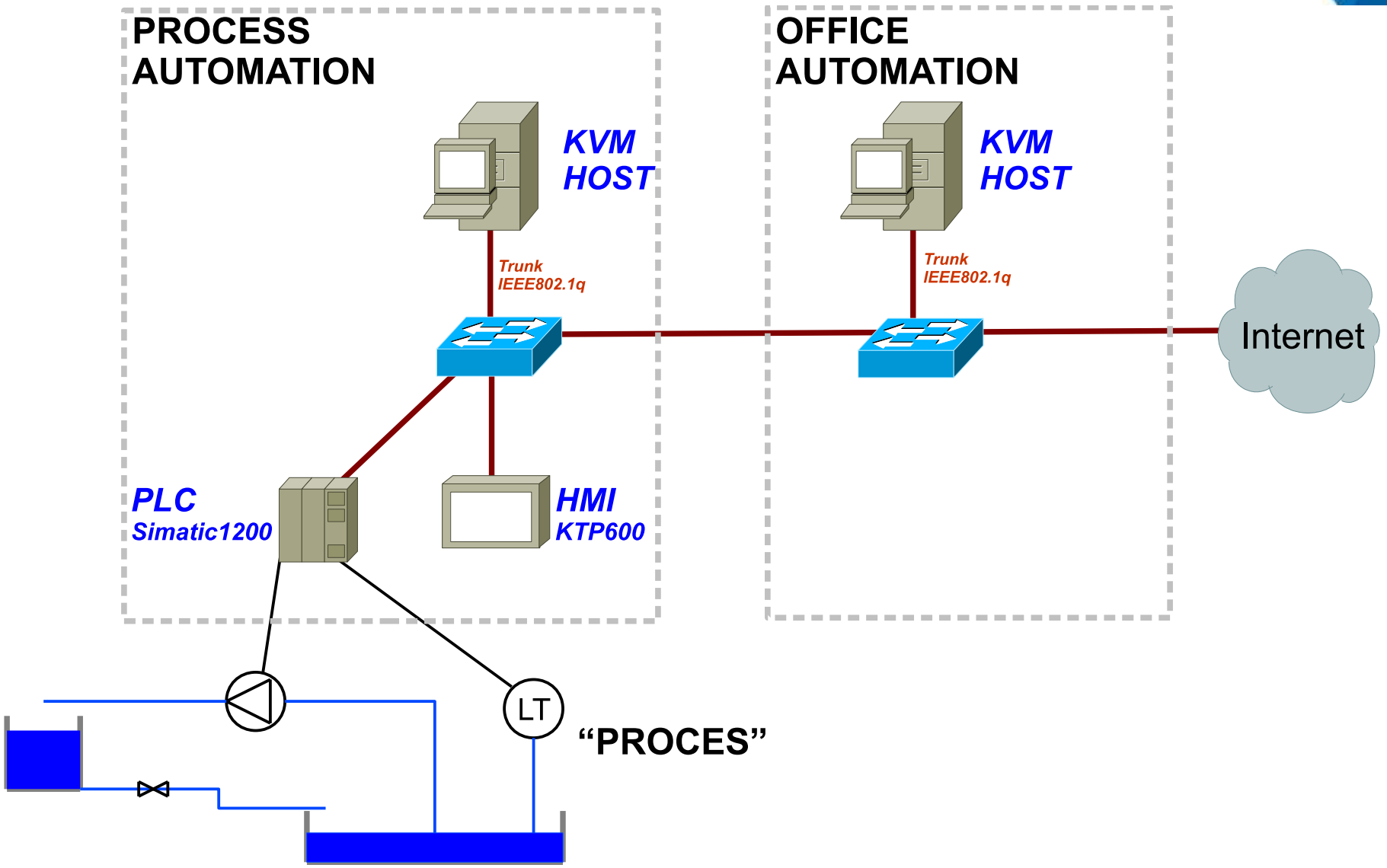
4. The Cyber Security Simulator

Example Attack Scenario:

- email with infected attachment
- infection of an office computer
- lateral movement towards ICS
- exploit of an ICS component
- process disruption



4. The Cyber Security Simulator (DESI)



5. Conclusions and future work

Results:

- Benchmark and its results (19 participants). Main results:
  - significant differences between the participants in protection
  - some of the vulnerabilities easy to solve by well-known controls
  - identification of cyber security dilemmas, related with patching, centralised control, and disaster recovery
- ICS cyber security simulator
  - used for feedback and awareness of observed vulnerabilities

Future work:

- adapting the benchmark to other ICS-related sectors
- further development of the cyber security simulator

Questions?

http://www.nu.nl/binnenland/3839880/waterschappen-pompen-nog-volop-wateroverlast.html