A Survey of Industrial Control System Testbeds

Hannes Holm

hannes.holm@foi.se

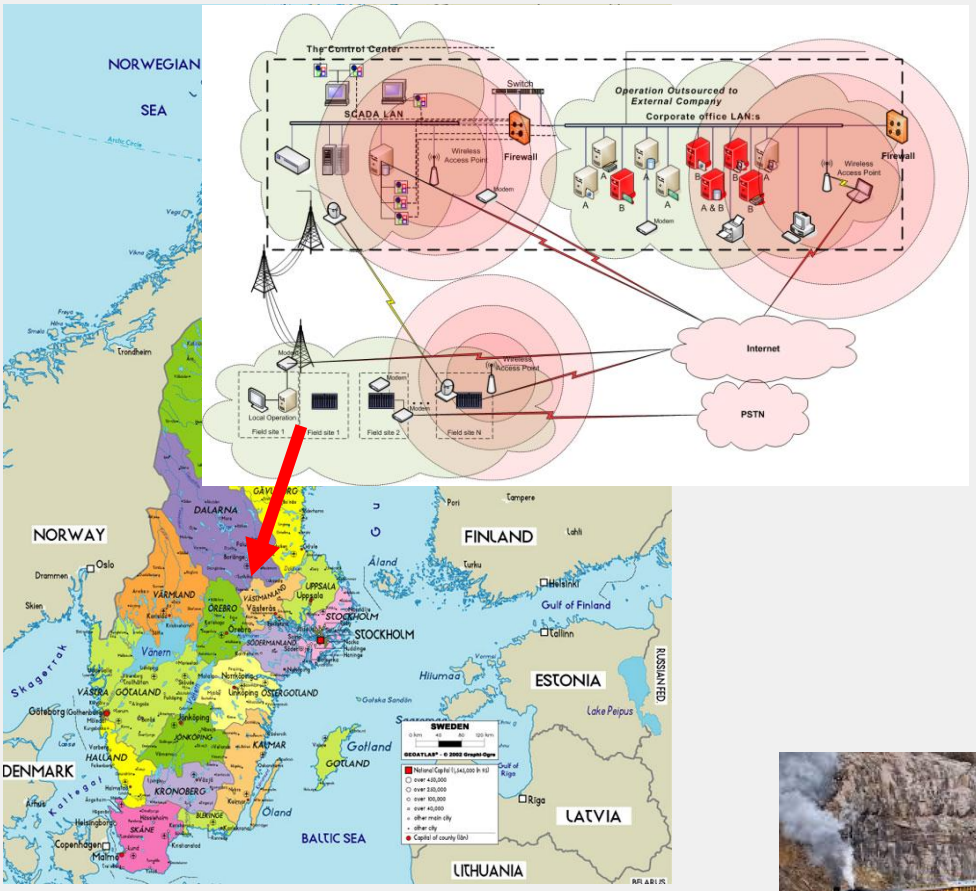
FOI

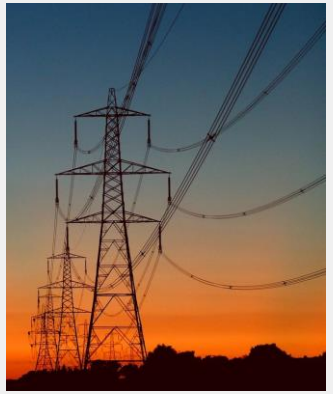
Background

- VICS, Virtual Industrial Control System testbed
- The Swedish part of a collaboration project involving
  - Funding: Swedish Civil Contingencies Agency (MSB) and Department of Homeland Security (DHS)
  - Execution: Swedish Defence Research Agency (FOI) and Idaho National Laboratory (INL)

- Pilot study can downloaded from (in English):
  - http://foi.se/rapport?rNo=FOI-R--4073--SE

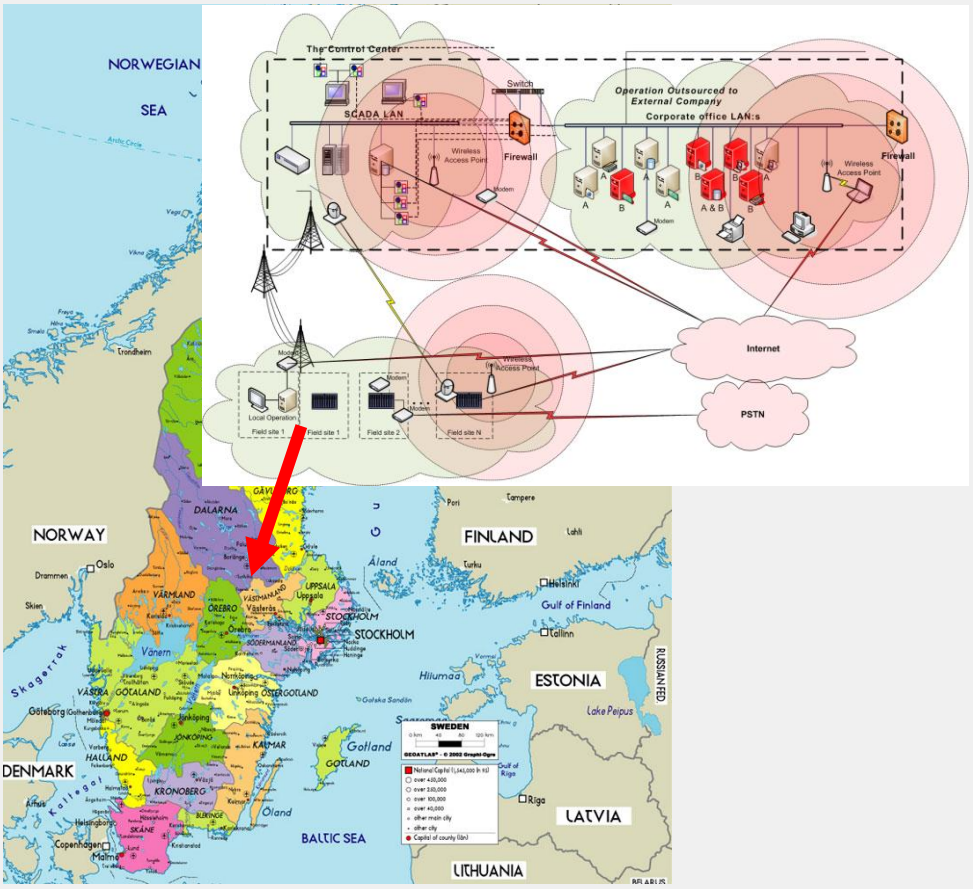
Background

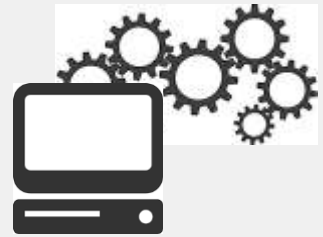




http://foi.se/rapport?rNo=FOI-R--4073--SE

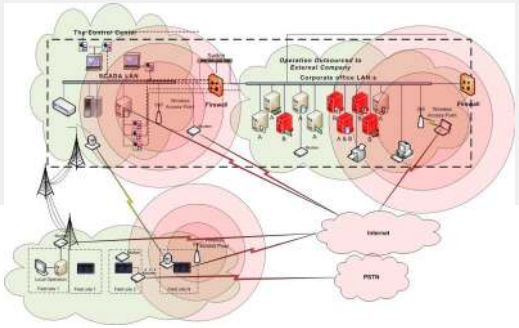
Background





Copy an operational system into a lab environment

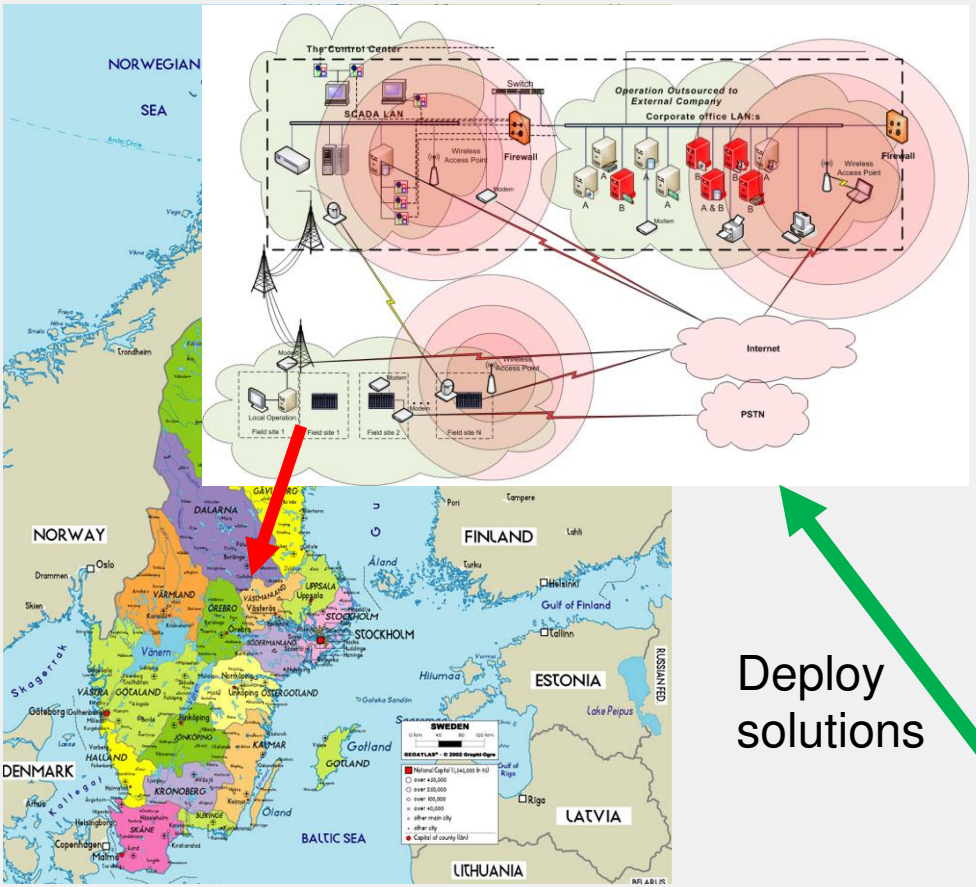
Perform automated vulnerability analysis



http://foi.se/rapport?rNo=FOI-R--4073--SE

FOI

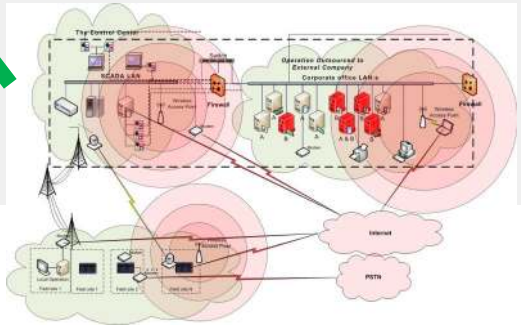
Background



Copy an operational system into a lab environment

Perform automated vulnerability analysis

Deploy solutions

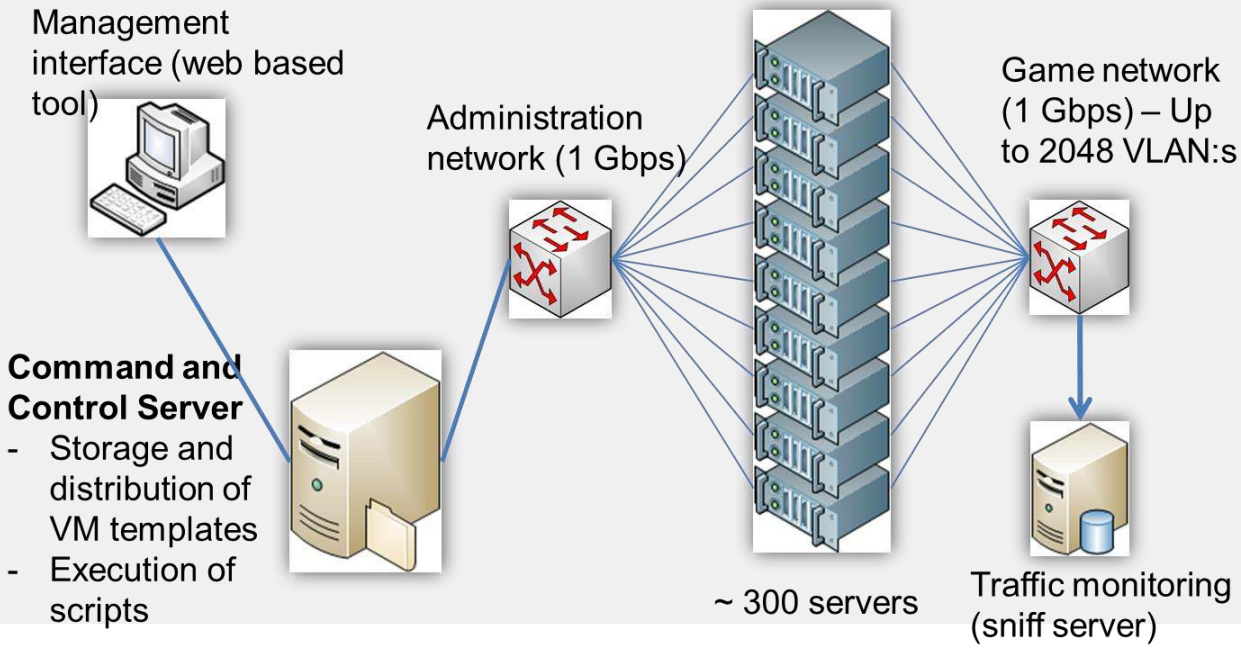


http://foi.se/rapport?rNo=FOI-R--4073--SE

FOI

Test environment at FOI

- Swedish national center for security in industrial information and control systems (NCS3)
- Cyber Range And Training Environment (CRATE)

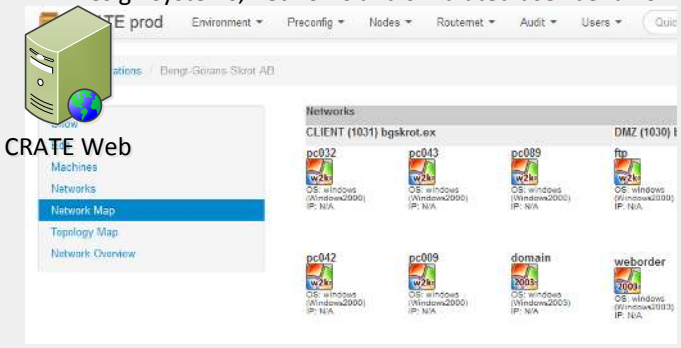


www.foi.se/crate

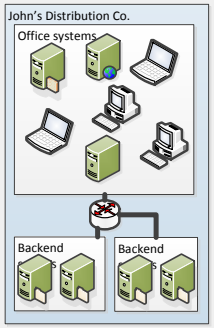
Test environment at FOI

- Cyber Range And Training Environment (CRATE)

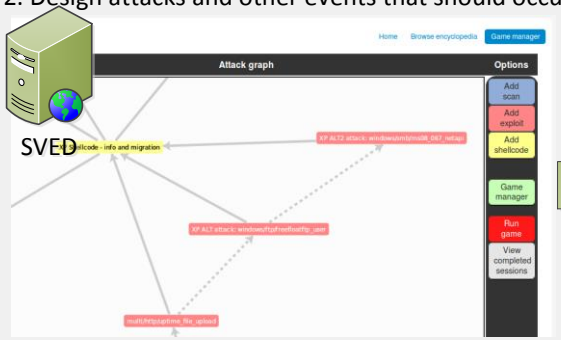
1. Design systems, networks and simulated user behavior



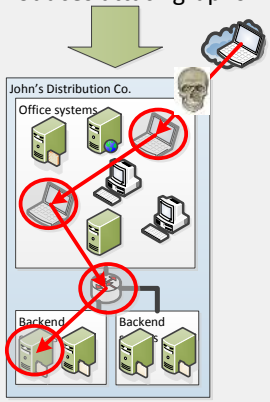
Produces a system design



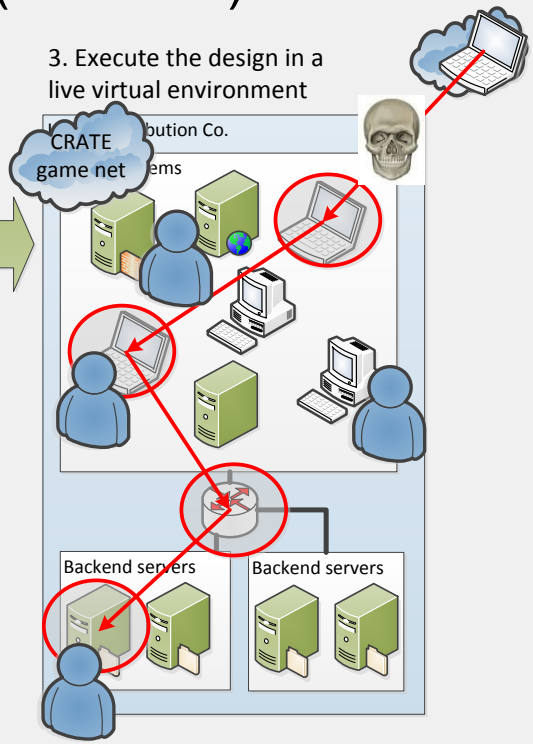
2. Design attacks and other events that should occur



Produces attack graphs



3. Execute the design in a live virtual environment



www.foi.se/crate

Surely, someone else must have done this before?

- RQ1: Which ICS testbeds have been proposed for scientific research?
- RQ2: Which research objectives do current ICS testbeds support?
- RQ3: How are ICS components implemented in current ICS testbeds?
- RQ4: How do existing ICS testbeds manage requirements?

http://foi.se/rapport?rNo=FOI-R--4073--SE

FOI

Systematic literature review

- Articles published in Scopus between January 2010 and the December 2014

RQ1

ID	University/Organization	Country	References
1	American University of Sharjah	Abu Dhabi	[11]
2	Queensland University of Technology	Australia	[30]
3	RMIT University	Australia	[2],[40]
4	Research Institute of Information Technology and Communication	China	[58]
5	Technical Assessment Research Lab	China	[17]
6	Tsinghua University of Beijing	China	[9]
7	University of Zagreb	Croatia	[28]
8	Queen's University Belfast	Ireland	[61]
9	University College Dublin	Ireland	[51]
10	European Commission Joint Research Centre	Italy	[20],[50]
11	European Commission Joint Research Centre	Italy	[16]
12	Ricerca sul Sistema Energetico	Italy	[14]
13	American University of Beirut	Lebanon	[44]
14	University Kuala Lumpur	Malaysia	[47],[48]
15	TNO	Netherlands	[8]
16	ITER Korea	South Korea	[54]
17	Case Western Reserve University	USA	[34]
18	Iowa State University	USA	[22],[23]
19	ITESM Campus Monterrey	USA	[43]
20	Lewis Research Center	USA	[4]
21	Mississippi State University	USA	[35],[36],[41], [42],[57]
22	Ohio State University	USA	[21]
23	Pacific Northwest National Laboratory	USA	[15]
24	Sandia National Laboratories	USA	[56]
25	Tennessee Technological University	USA	[52]
26	The University of Tulsa	USA	[24]
27	UC Berkeley	USA	[18]
28	University of Arizona	USA	[33]
29	University of Illinois at Urbana-Champaign	USA	[6],[7],[12]
30	University of Louisville	USA	[26]

FOI

RQ2: Testbed objectives

Table 2: Objectives of testbeds.

Objective	Testbeds
Vulnerability analysis	16
Education	9
Tests of defense mechanisms	9
Power system control tests	4
Performance analysis	1
Creation of standards	1
Honeynet	1
Impact analysis	1
Test robustness	1
Tests in general	1
Threat analysis	1

RQ3: Testbed implementation choices

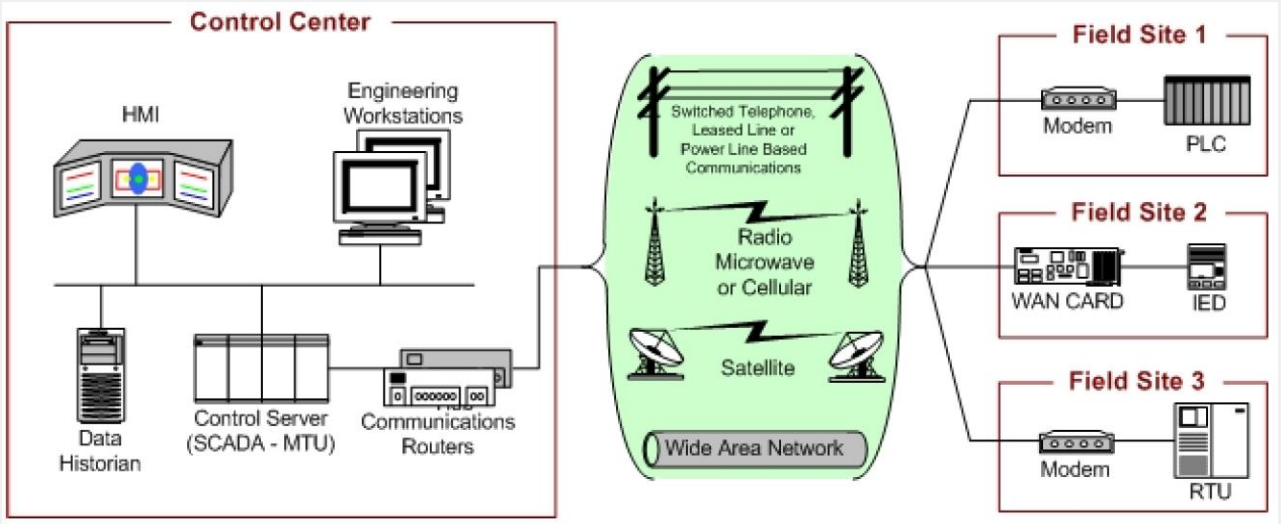


Table 3: Number of articles assessing different areas and methods of implementation (virtualization, emulation, simulation and hardware).

Area	Covered	Virtualization	Simulation	Emulation	Hardware
Control center	20	4	9	1	11
Communication architecture	22	6	10	3	11
Fields devices	23	0	14	0	14
Physical process	12	0	12	0	0

RQ4: Testbed requirements (fidelity)

Table 4: Testbed fidelity.

Fidelity	Testbeds
Not covered	19
Study of real systems	7
Based on standards	4

- Few metrics presented
  - Modbus traffic (e.g., byte throughput, error count and packet size)
  - Execution time of testbed to the required execution time of physical processes
- Data collection only discussed by a single paper

FOI

Future work (for academia)

- Clearly state the objectives of the testbed and relate these objectives to the configuration of the testbed
- Employ virtualization or emulation in front of simulation and hardware approaches
- Provide empirical results describing how the testbed fulfills its stated requirements

FOI

Future work (for us)

- Involve ICS developers and opererators
- Identify testbed requirements
- Design metrics for measuring fulfillment of requirements
- Develop and adapt tools and methods for capturing the configurations of operational ICS systems
- Develop and adapt tools and methods for simulating, virtualizing and emulating ICS components and configurations
- Develop and adapt tools and methods for vulnerability discovery in ICS systems

FOI