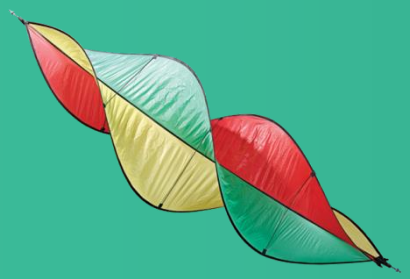
KU LEUVEN

TECHNOLOGIECAMPUS GENT



Een Tool voor Analyse van Veiligheid in Industriële Controlesystemen

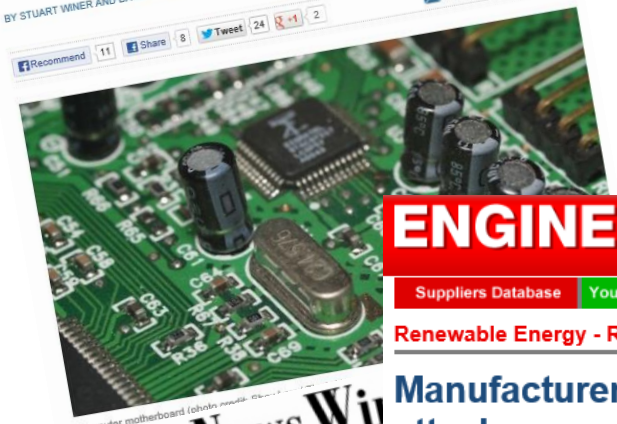
Laurens Lemaire

15/03/2016

‘Stuxnet virus attacked Iran earlier than thought’

Researchers uncover previously unknown version of the malicious program that sabotaged Natanz nuclear facility in 2010

BY STUART WINER AND DAVID SHAMAH | February 27, 2013, 11:56 am



Computer motherboard

Security Affairs

Read, think, share ... Security is everyone's responsibility

Intelligence | Laws and regulations | Malware | Security | Social Networks

TAGS

brute force, Cyber attacks, cyber espionage, ICS-CERT, spear phishing, SQL injection, watering hole

ICS-CERT Surge In attacks against Energy Industry

by paganinip on July 2nd, 2013

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

AIChE

about | careers | video | fun

– Turning SCADA into NADA

As the Internet of things quickly expands throughout the energy sector, with millions of machines and sensors communicating throughout company networks and over the Internet, the security

ENGINEERLIVE

INTERNATIONAL MINING ENGI

Suppliers Database | Your Career | Search this site

Renewable Energy - Renewable Energy

Manufacturers warn of rising cyber security attacks

Leading British manufacturers have united to warn that businesses are facing a rapidly growing threat from deliberate industrial security breaches, noting that the sector needs to increase investment to ensure that industrial safety remains a top priority

GCN

Technology, Tools and Tactics f

BIG DATA | CLOUD | CYBERSECURITY | DATA CENTERS | EMERGING TECH | MOB

Industrial control 'honeypots' show systems are under attack

By Kevin McCaney | Aug 07, 2013

Security experts have been warning for years that industrial control systems (ICS) are vulnerable to cyberattacks, but a recent work with ICS "honeypots" shows just how actively they're being probed and attacked.

Kyle Wilhoit, a threat researcher at Trend Micro, demonstrated at last week's Black Briefings in Las Vegas how he set up 12 honeypots in eight countr and recorded 74 attacks on them between Marc Technology Review how he

omeland Security News Wi

HOMETRICS | BORDERS | BUSINESS | CYBERSECURI

INFRASTRUCTURE | PUBLIC SAFETY | PUBLIC HEALTH | SCI-TEC

100% ONLINE MASTER OF SCIENCE Legal Studies

• Homeland Security
• Criminal Justice
• Law & Public Policy

CAL

Infrastructure protection

DHS: Industrial control systems su to 200 attacks in 2012

Share

Published 14 January 2013

A DHS report released last week revealed that industr systems, which are used to monitor and control criti infrastructure facilities, were hit with 198 document cyberattacks in 2012, and that many of these attacks were serious.

A DHS report released last week revealed that industrial co which are used to monitor and control critical infrastructu hit with 198 documented cyberattacks in 2012, and that m attacks were serious.

Forty percent of those attacks were on energy firms, acco Industrial Control Systems (ICS) and Cyber Emergency R which reviewed every incident. Water utilities c attacks focused on them.

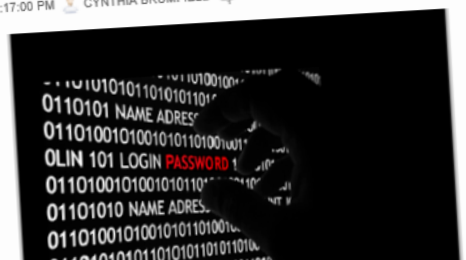
DigitalCrazyTown

Technology, policy and business analysis covering the media, Internet, broadband, mobile and smart grid arenas.

HOME | ABOUT | THINK SOMETHING'S CRAZY? | DCT ASSOCIATES

Cybersecurity Experts: It's Child's Play to Attack Energy Industrial Control Systems

4/09/2013 04:17:00 PM | CYNTHIA BRUMFIELD | NO COMMENTS

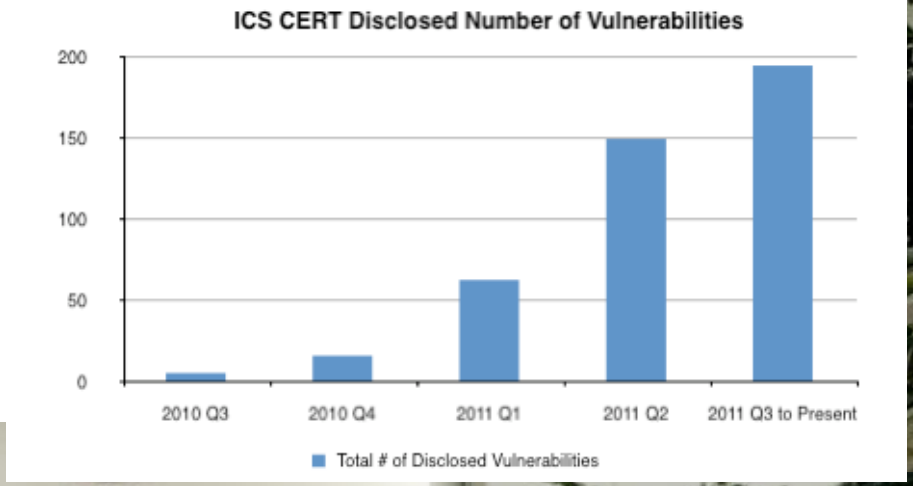


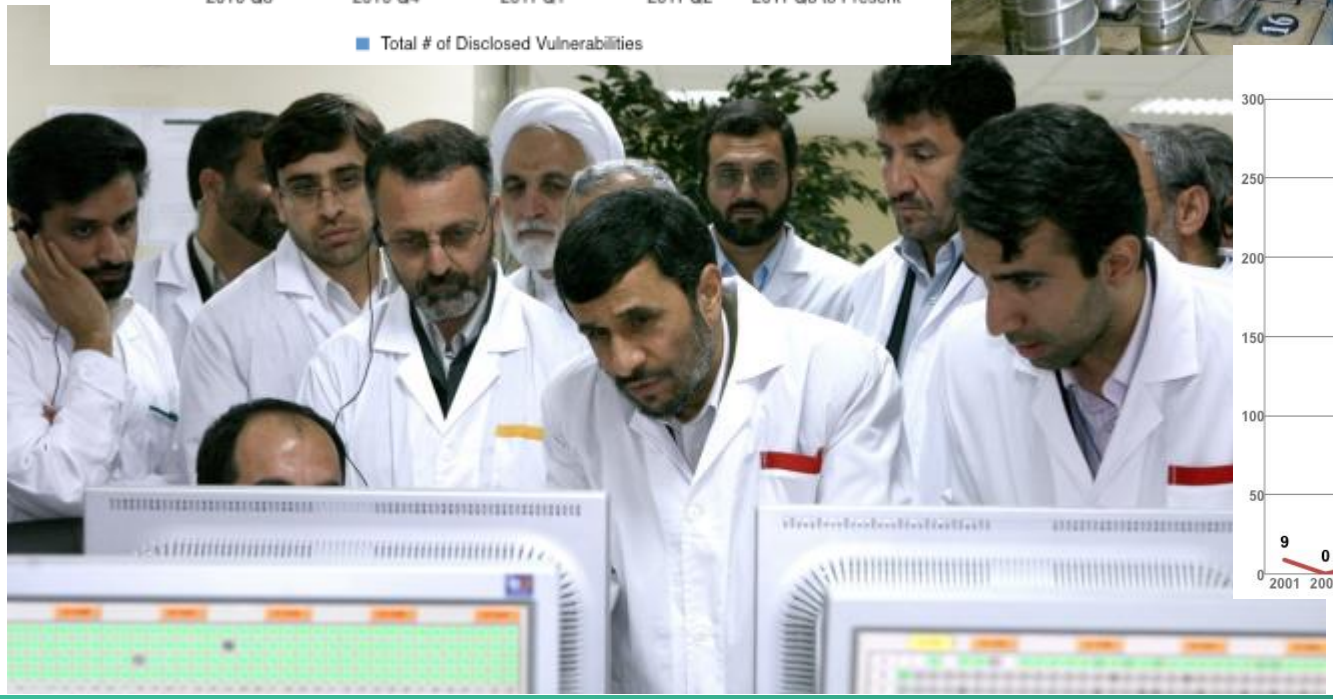
ading decision renewable energy, food/beverage

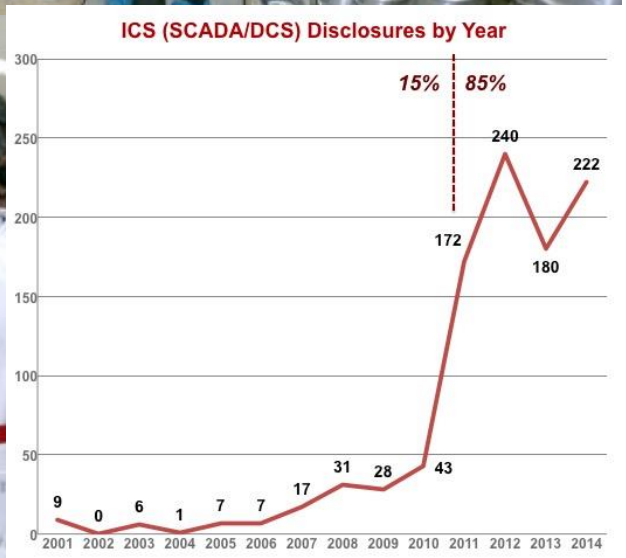
plants and critic eive the threat nt) said that eing subjecte

acking is no strial scale our survey growing. has bee more tin ity of pl cks w

2010 - Stuxnet







KU LEUVEN

2015 - Ukrainian Grid Hack

- Multiple power distribution centers
- BlackEnergy & KillDisk
- Denial of Service
- Russian hackers?

12/24/2015

Dear customers!

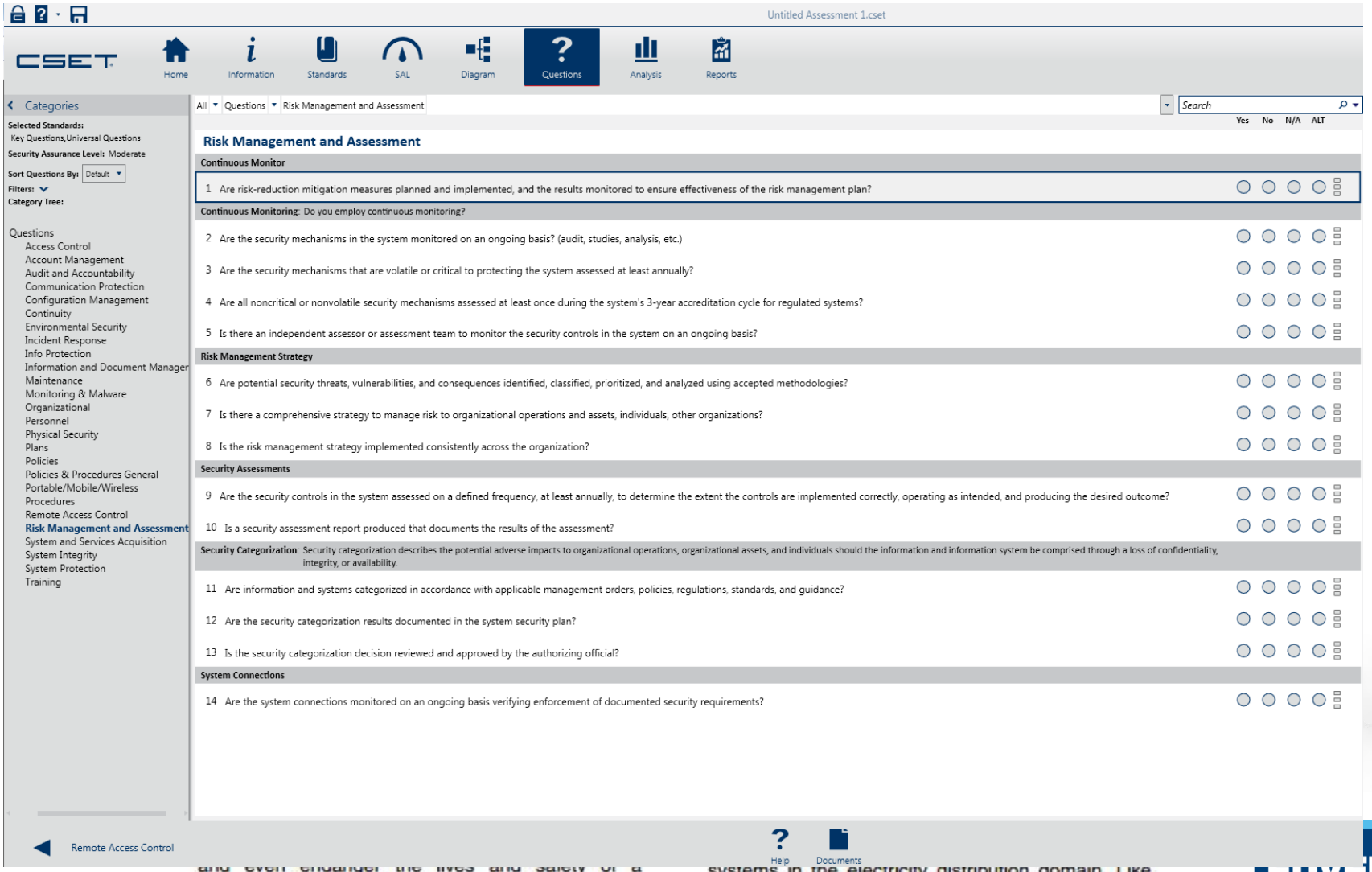
23 December 2015 there was a technical failure in the infrastructure, making it difficult to dial call center PJSC "Kyivoblenergo."

We apologize for any inconvenience.

KU LEUVEN

Prc

DOI: http://dx.doi.org/10.14236/ewic/ICS2015.2



population. Failures of critical infrastructure can be caused by different events, such as natural catastrophes (e.g., flooding), equipment malfunction

systems in the electricity distribution domain. Like many of these standards, it is not a revolution, but a careful evolution, to address security issues without completely breaking backwards-compatibility and

Goal

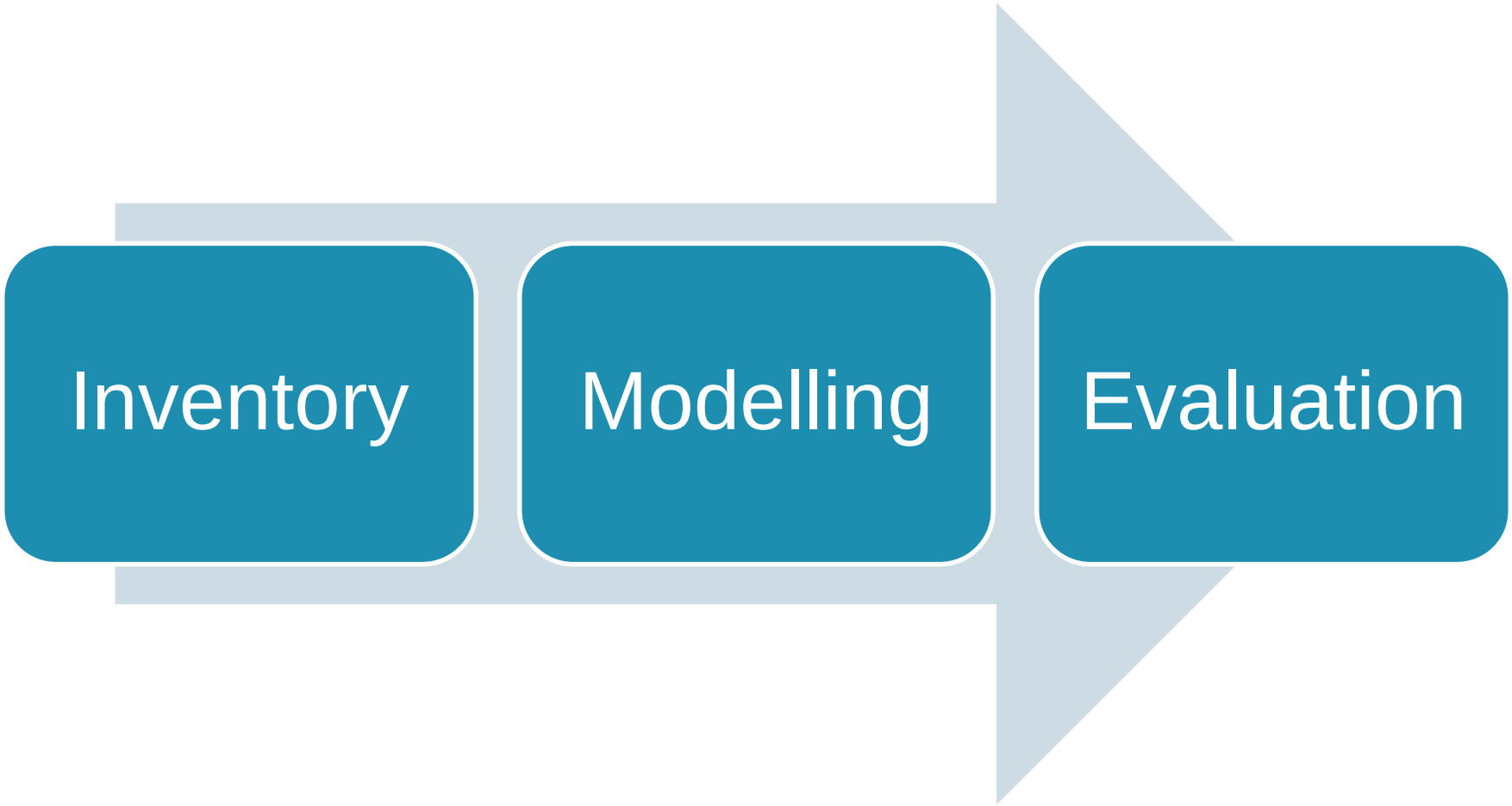
- Tool for the analysis of security in ICS
  - As automated as possible
  - Quick to reuse after changes or new vulnerabilities
  - Useful feedback

KU LEUVEN

The Tool

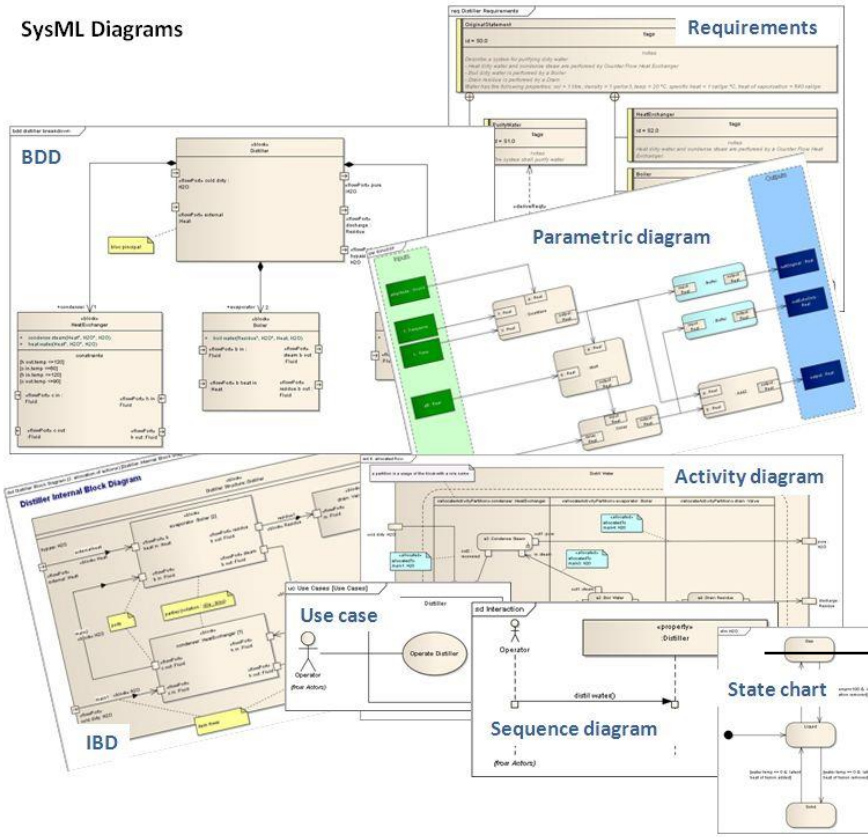
- Modelling approach
  - SysML
  - No system disturbance
- Logic-based reasoning
  - IDP3
- Text-based output

“As automated as possible”



KU LEUVEN

Methodology



INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

NIST

Component Vulnerabilities

Security Best Practices

Model

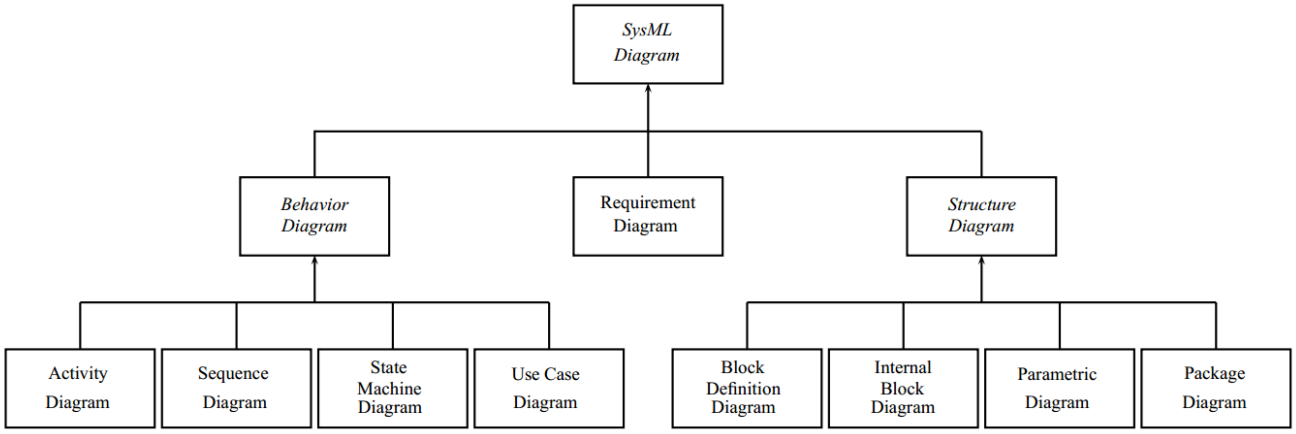
IDP³

Conclusions

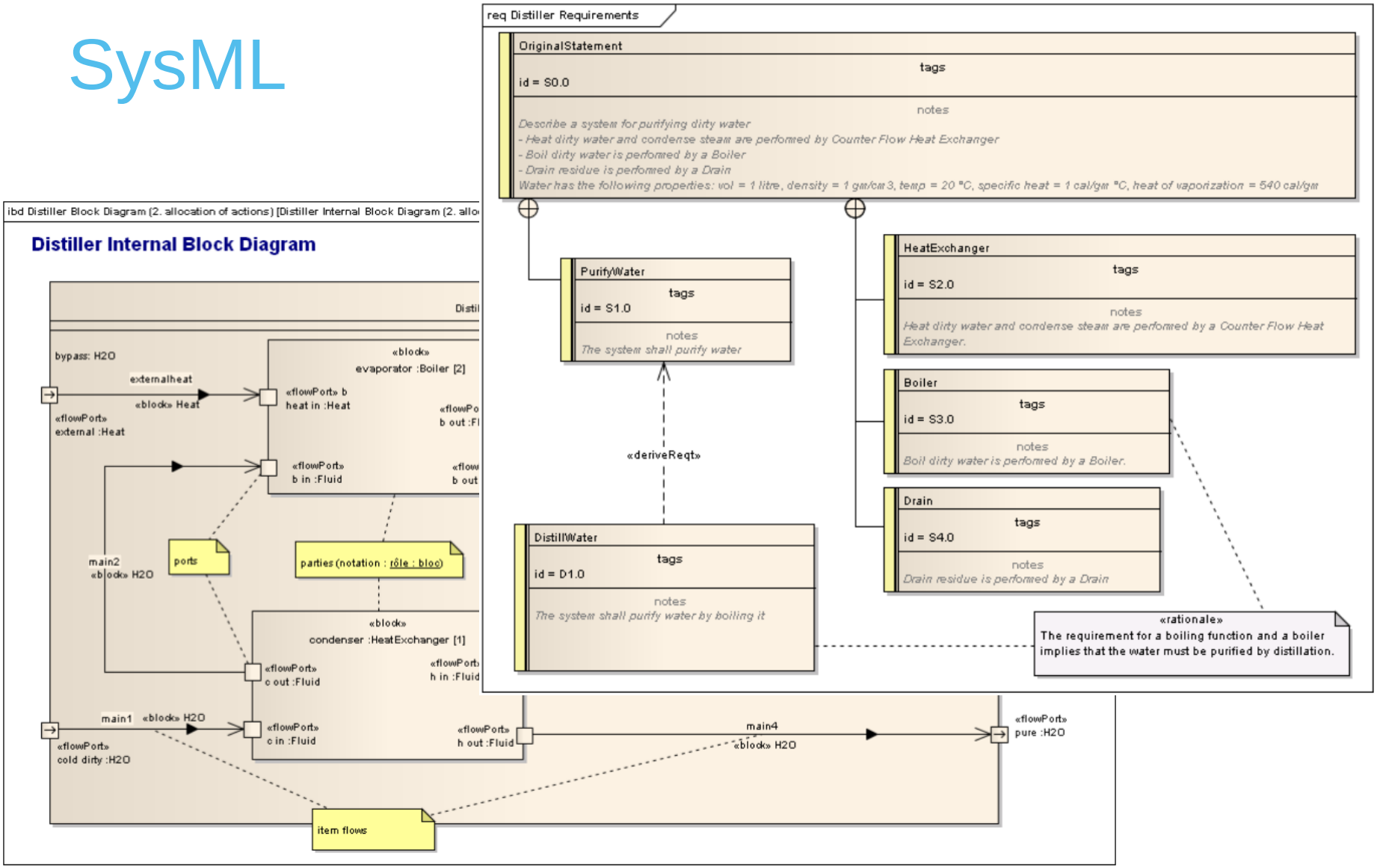
KU LEUVEN

SysML

- Systems Modeling Language
- Extension of UML
- Model-Based Systems Engineering
- “Supports specification, analysis, design, verification and validation of systems and systems-of-systems.”
- Contains nine diagrams:



SysML

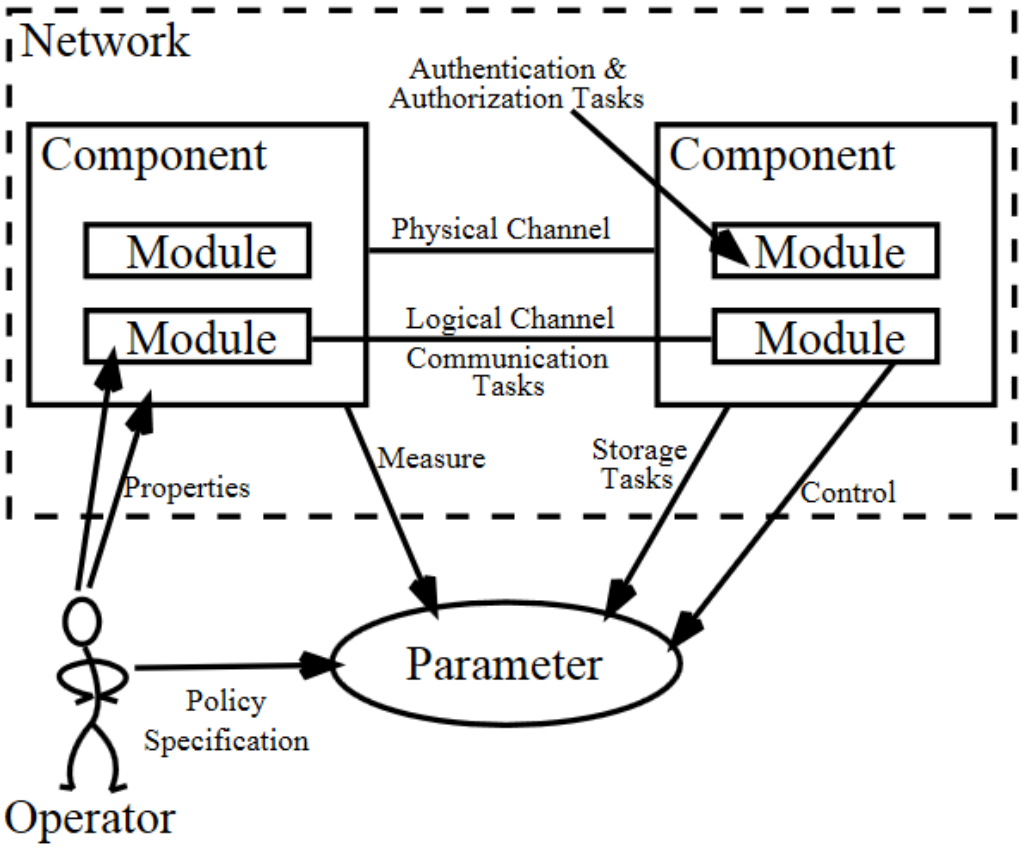


KU LEUVEN

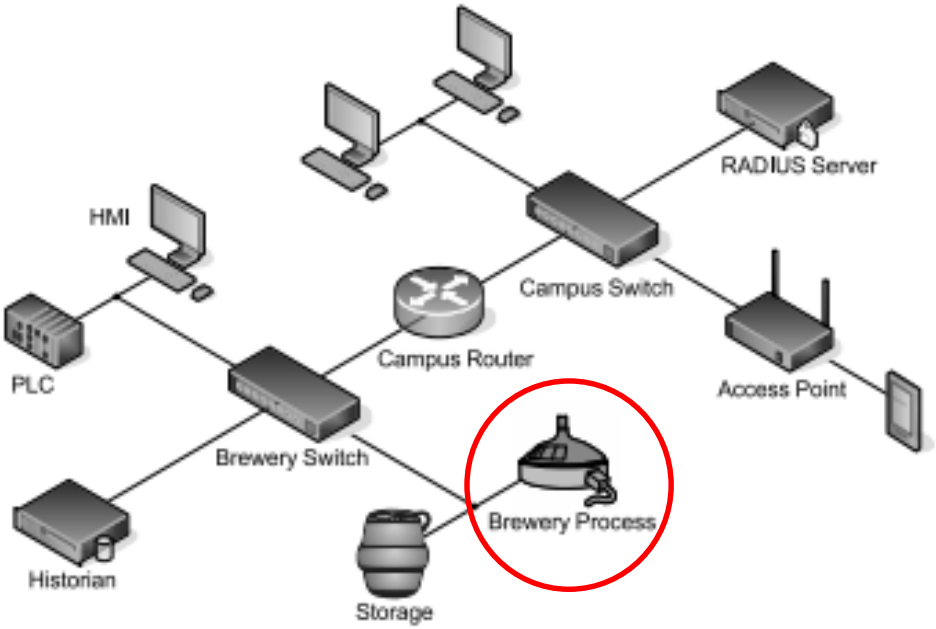
IDP 3

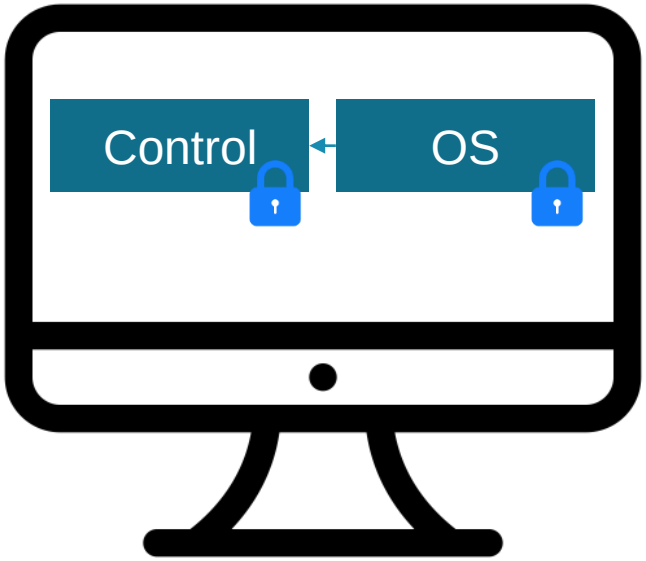
- Imperative Declarative Programming framework
- Extension of first order logic
  - Inductive definitions
  - Aggregates
  - Partial functions
  - …
- IDP instance consists of:
  - Vocabulary
  - Theory
  - Structure
- Solves search problems using model expansion

Model - Conceptual



Model - Example





ICS-CERT

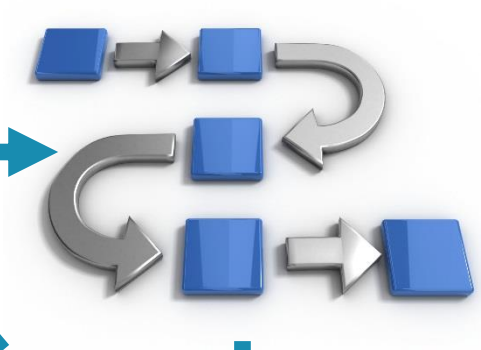
ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Vulnerability Database
  - Alerts
  - Advisories
- Department of Homeland Security
- Vulnerabilities added to input model

KU LEUVEN

Feedback



Component vulnerabilities
ICS CSR 2

System vulnerabilities
ICS CSR 3

Simulations
(JISA Journal)

KU LEUVEN

Limitations

- Approach
  - Zero-day attacks
  - Based on system model
- Tool
  - Currently focus on SCADA systems
  - Feedback
  - Vulnerability database management

Case Study - Operational System

- Industrial environment
- 16 processes
  - Touchscreen HMI + PLC
  - Various sensors and actuators
- Switches
- Industrial SCADA PC

Case Study

- Users
  - Technicians
    - Monitor parameters
    - Reset alarms
  - Operators
    - Modify parameters
  - Managers
    - Change passwords
    - Export data
  - Manufacturers
    - Additional information for remote assistance

KU LEUVEN

Input Model

- User Model
  - *Type User*
  - *User = {Technician, Operator, Attacker…}*
  - *HasToken(User, Token)*
- Policy Specification
  - *Permission(User, Parameter, Operation)*

	$Temp_{S_1}$	$Alarm_{S_1}$	$Humidity_{S_2}$
$Technician$	R	$R\ M$	R
$Operator$	$R\ M$	$R\ M$	$R\ M$
$Manager$	$R\ M$	$R\ M$	$R\ M$
$Attacker$			

Evaluation

$$\left\{ \forall u, p, c : (ChangeConfig(u, c) \wedge ConfigAffects(c, p)) \Rightarrow Permission(u, p, "Modify"). \right\}$$

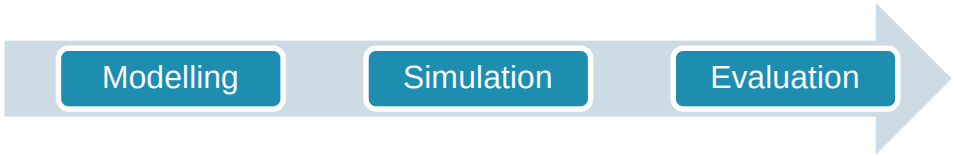
IDP Listing 2: The IDP query that was not satisfied

```
>>> Generating an unsatisfiable subset of the given theory.
>>> Unsatisfiable subset found, trying to reduce its size (might take some time,
can be interrupted with ctrl-c.
The following is an unsatisfiable subset, given that functions can map to at most
one element (and exactly one if not partial) and the interpretation of types and
symbols in the structure:
(~(ChangeConfig("Technician","ConfigurationS1") &
ConfigAffects("ConfigurationS1","TempS1")) | (
Permission("Technician","TempS1","Modify"))) instantiated from line 360
with c="ConfigurationS1", p="TempS1", u="Technician".
Elapsed time to find models : 2.24 sec
```

IDP Listing 3: The final lines of the output, showing the trace of the failed model

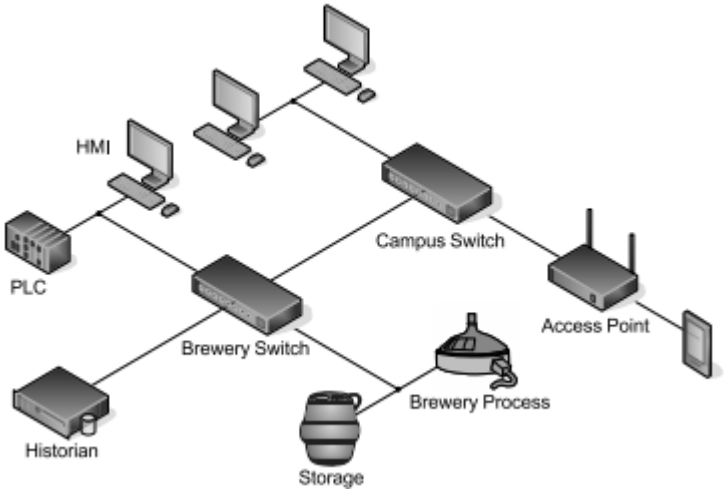
Case Study - Simulations

- Using our tool in the design phase of your system

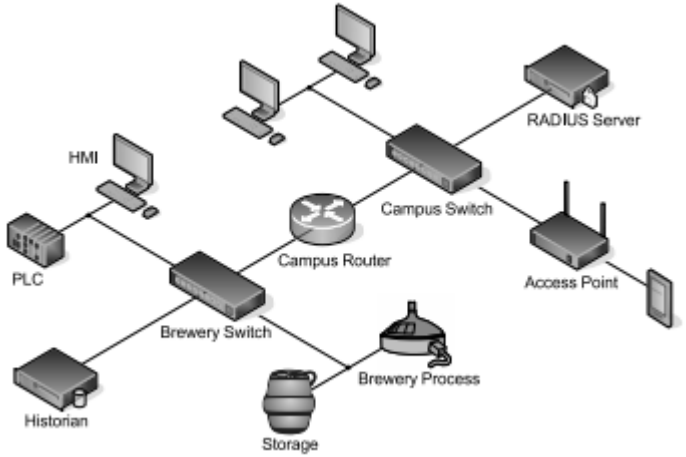


- Test different kinds of architectures
  - Simulate the effects of attacks or components failing
- Case study: brewery
  - Connect the brewery to the campus network
  - Three different architectures
  - Several simulations

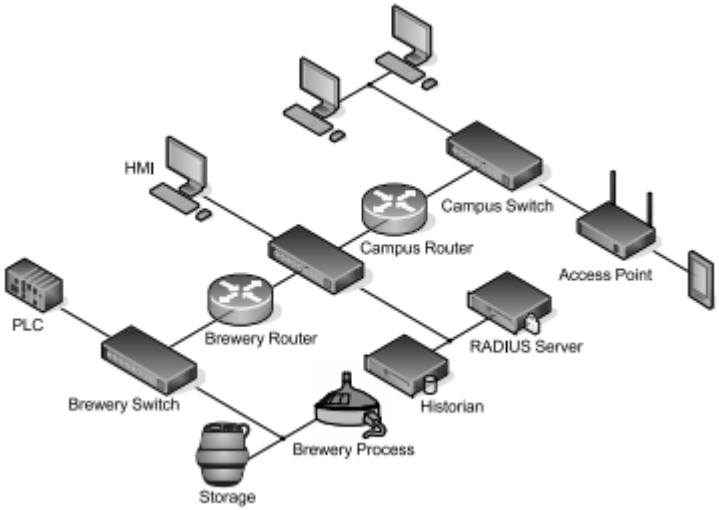
Architectures



Architectures



Architectures



Evaluation

- Simulations
  - User rights
  - Compromised components

```
CompromisedPermission :
{ "Attacker","CTT",Modify; "Attacker","CTT",Read; "Attacker",
"PF",Modify; "Attacker", "PF",Read; "Student","CTT",Modify;
"Student","PF",Modify }
>>> Generating an unsatisfiable subset of the given theory.
>>> Unsatisfiable subset found, trying to reduce its size
(might take some time, can be interruptedwith ctrl-c.
The following is an unsatisfiable subset, given that functions
can map to at most one element (and exactly one if not partial)
and the interpretation of types and symbols in the structure:
((? x[Module] : ModifyParameter("Student",x[Module],"PF"))
=> Permission("Student","PF","Modify")) instantiated from
line 396 with u="Student", z="PF".
Elapsed time to find models : 1.02 sec
```

KU LEUVEN

Conclusion

- Tool to analyse security of ICS
  - Modelling approach
  - As automated as possible
  - Logic-based
    - Vulnerability databases
    - Standards, guidelines and papers
- 2 Case studies

KU LEUVEN

Questions?

KU LEUVEN