

Een Tool voor Analyse van Veiligheid in Industriële Controlesystemen

Laurens Lemaire

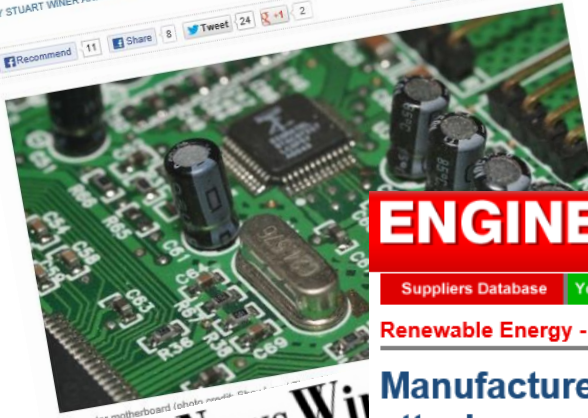
15/03/2016

'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, 11:55 am | 0

Recommend 11 | Share 8 | Tweet 24 | +1 2 | Email | Print | Share



Computer motherboard (shutterstock.com)

Homeland Security News Wire

100% ONLINE
MASTER OF SCIENCE
Legal Studies

• Homeland Security
• Criminal Justice
• Law & Public Policy

INFRASTRUCTURE PUBLIC SAFETY PUBLIC HEALTH SCI-TEC

OMETRICS BORDERS BUSINESS CYBERSECURITY

CAL GLOBAL

100% ONLINE
MASTER OF SCIENCE
Legal Studies

Infrastructure protection

DHS: Industrial control systems su to 200 attacks in 2012

Published 14 January 2013

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

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

Forty percent of those attacks were on energy firms, according to the report. Forty percent of those attacks were on energy firms, according to the report. Forty percent of those attacks were on energy firms, according to the report.

ENGINEERLIVE

Suppliers Database Your Career

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

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



Security Affairs

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

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

ICSCERT Surge In attacks against Energy Industry

by paganiip on July 2nd, 2013

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

Connected

AICHe™ Where chemists connect

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 needs of these devices are also expanding.

GCN

Technology, Tools and Tactics for the Energy Industry

Share Like 3 Tweet +1

BIG DATA CLOUD CYBERSECURITY DATA CENTERS EMERGING TECH MOBILE



Industrial control 'honeypots' show systems are under attack

By Kevin McCaney | Aug 07, 2013

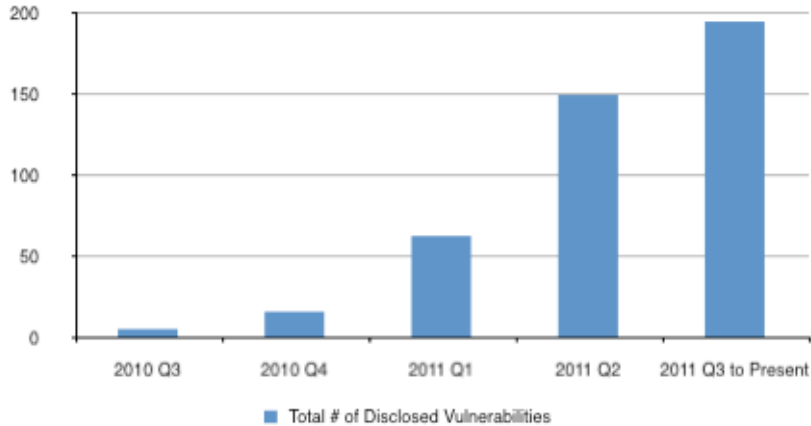
Security experts have been warning for years that industrial control systems (ICS) are vulnerable to cyberattacks, but a recent work with ICS "honeypots" shows just how actively they're being probed and attacked.

Kyle Wilhoit, a threat researcher at Trend Micro, demonstrated at last week's Black Hat conference in Las Vegas how he set up 12 honeypots in eight countries and recorded 74 attacks on them between March and May.

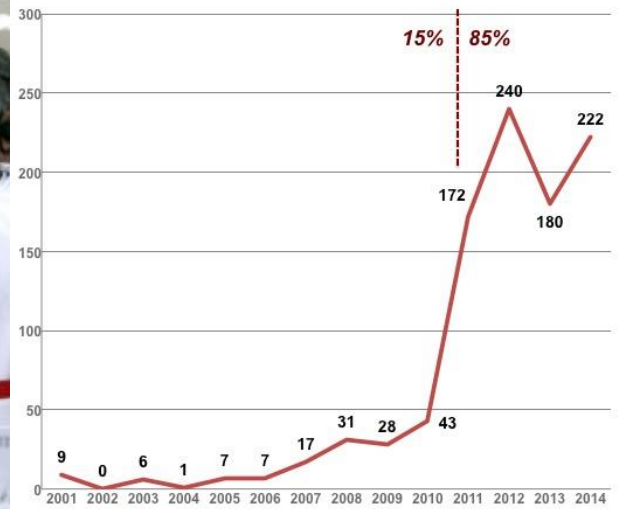
Technology Review how he set up 12 honeypots in eight countries and recorded 74 attacks on them between March and May.

2010 - Stuxnet

ICS CERT Disclosed Number of Vulnerabilities



ICS (SCADA/DCS) Disclosures by Year



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.



Untitled Assessment 1.cset

CSET Home Information Standards SAL Diagram Questions Analysis Reports

Categories: Selected Standards: Key Questions, Universal Questions Security Assurance Level: Moderate Sort Questions By: Default Filters: Category Tree: Questions Access Control Account Management Audit and Accountability Communication Protection Configuration Management Continuity Environmental Security Incident Response Info Protection Information and Document Management Maintenance Monitoring & Malware Organizational Personnel Physical Security Plans Policies Policies & Procedures General Portable/Mobile/Wireless Procedures Remote Access Control Risk Management and Assessment System and Services Acquisition System Integrity System Protection Training

All Questions Risk Management and Assessment Search Yes No N/A ALT

Risk Management and Assessment

Continuous Monitor

1 Are risk-reduction mitigation measures planned and implemented, and the results monitored to ensure effectiveness of the risk management plan?

Continuous Monitoring: Do you employ continuous monitoring?

2 Are the security mechanisms in the system monitored on an ongoing basis? (audit, studies, analysis, etc.)

3 Are the security mechanisms that are volatile or critical to protecting the system assessed at least annually?

4 Are all noncritical or nonvolatile security mechanisms assessed at least once during the system's 3-year accreditation cycle for regulated systems?

5 Is there an independent assessor or assessment team to monitor the security controls in the system on an ongoing basis?

Risk Management Strategy

6 Are potential security threats, vulnerabilities, and consequences identified, classified, prioritized, and analyzed using accepted methodologies?

7 Is there a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations?

8 Is the risk management strategy implemented consistently across the organization?

Security Assessments

9 Are the security controls in the system assessed on a defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome?

10 Is a security assessment report produced that documents the results of the assessment?

Security Categorization: Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability.

11 Are information and systems categorized in accordance with applicable management orders, policies, regulations, standards, and guidance?

12 Are the security categorization results documented in the system security plan?

13 Is the security categorization decision reviewed and approved by the authorizing official?

System Connections

14 Are the system connections monitored on an ongoing basis verifying enforcement of documented security requirements?

Remote Access Control Help Documents

and even endanger the lives and safety of a 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

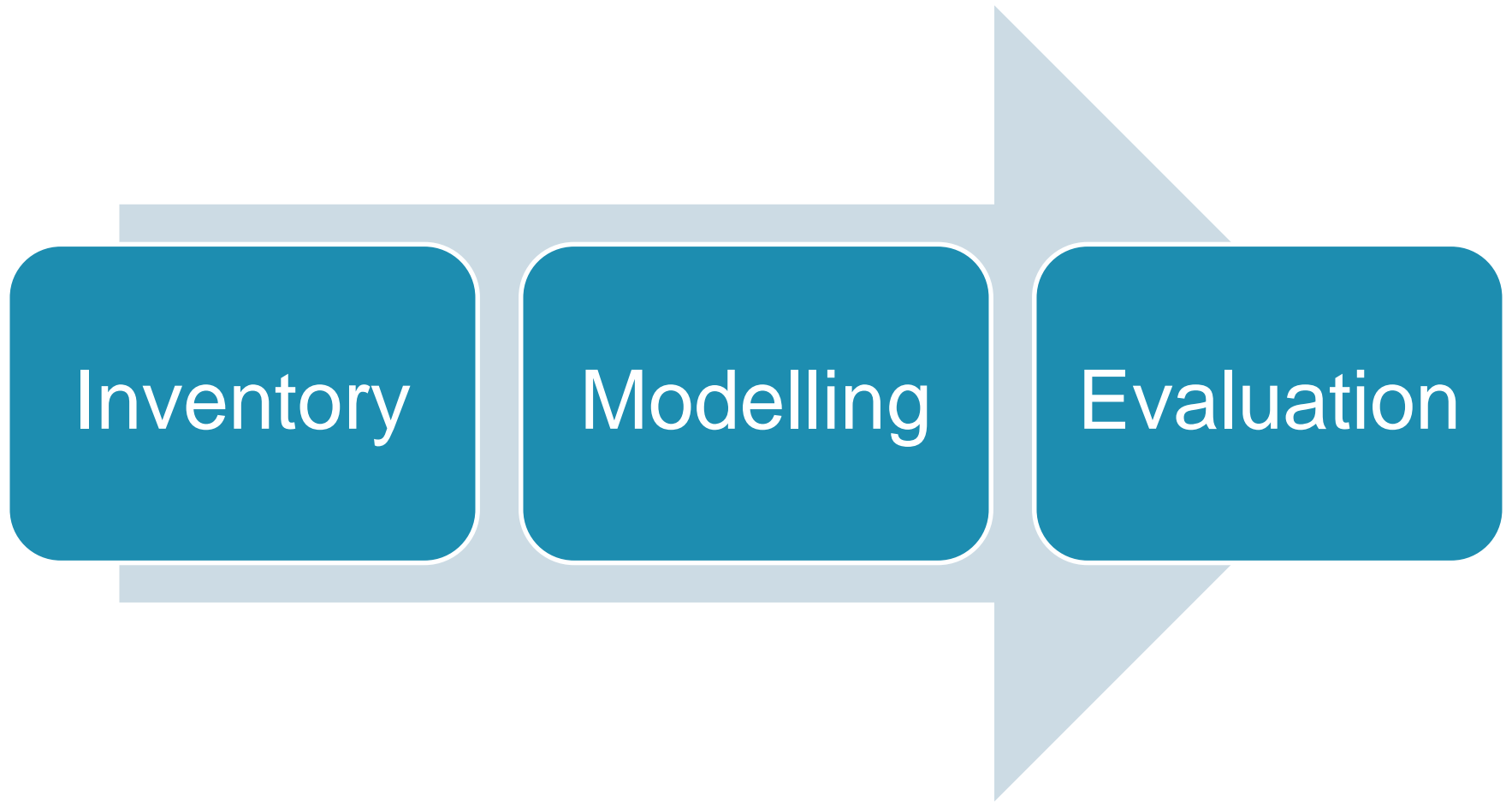


The Tool

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

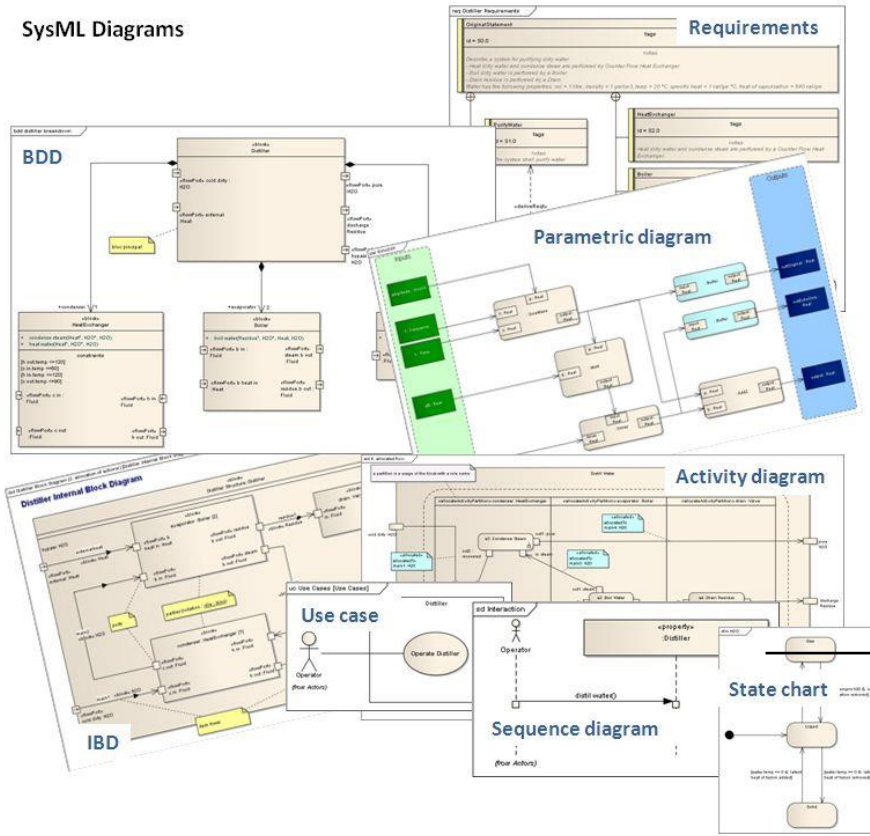


“As automated as possible”



Methodology

SysML Diagrams



INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

NIST

Component
Vulnerabilities

Security
Best Practices

Model

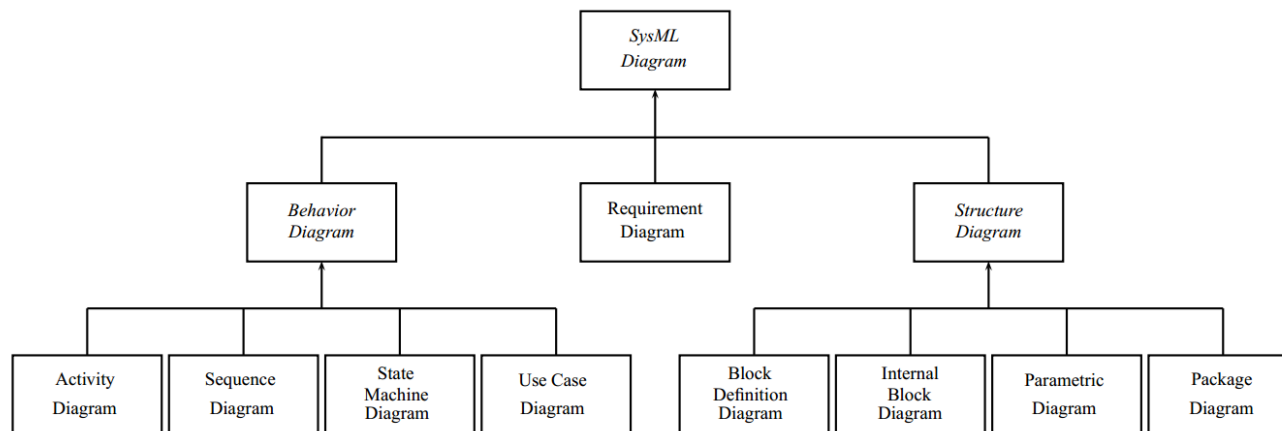
IDP³

Conclusions



SysML

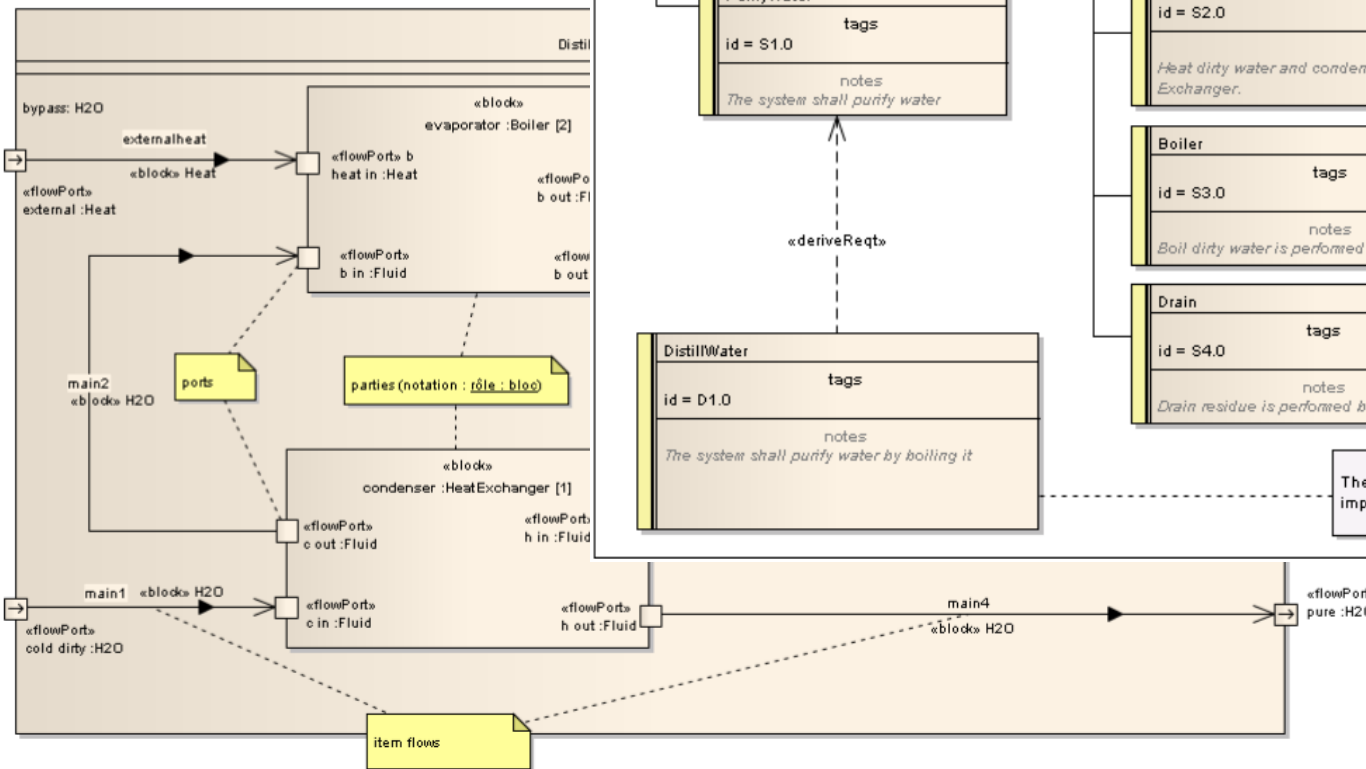
- Systems Modeling Language
- Extension of UML
- Model-Based Systems Engineering
- “Supports specification, analysis, design, verification and validation of systems and systems-of-systems.”
- Contains nine diagrams:



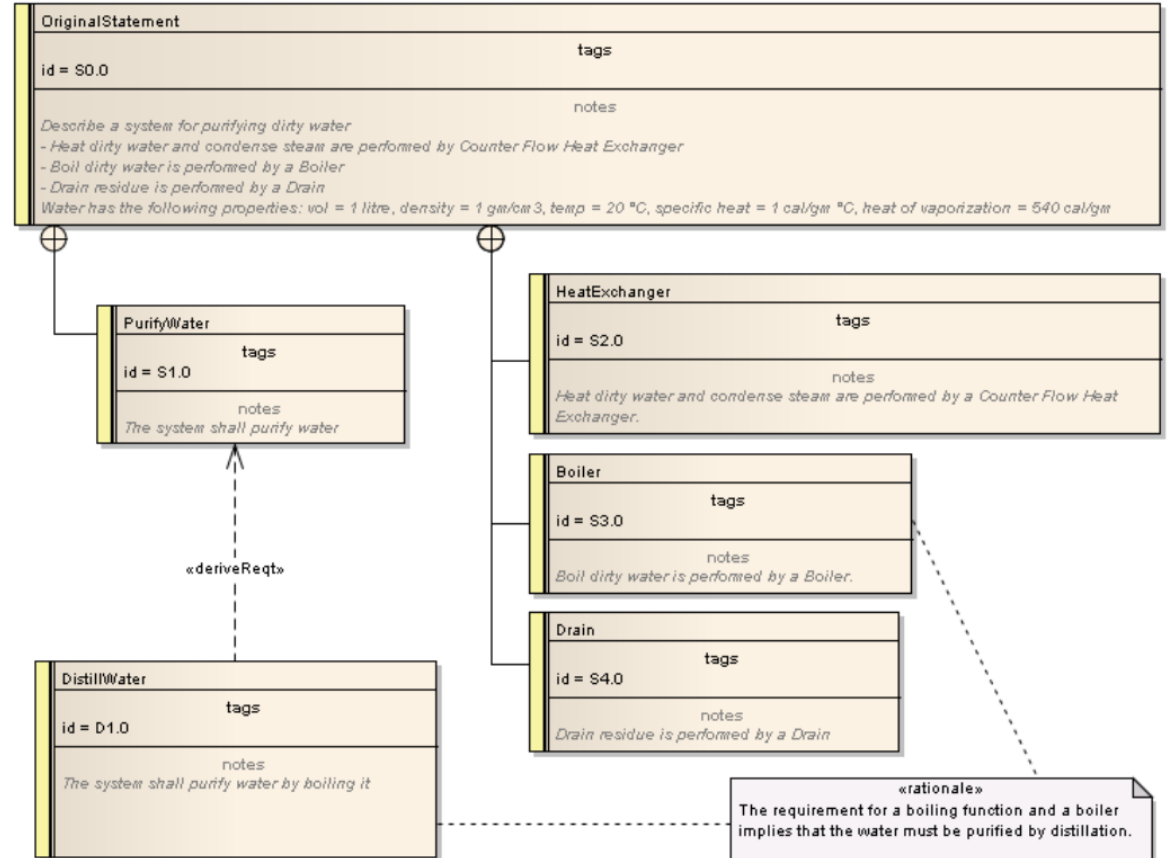
SysML

ibd Distiller Block Diagram (2. allocation of actions) [Distiller Internal Block Diagram (2. allo

Distiller Internal Block Diagram



req Distiller Requirements

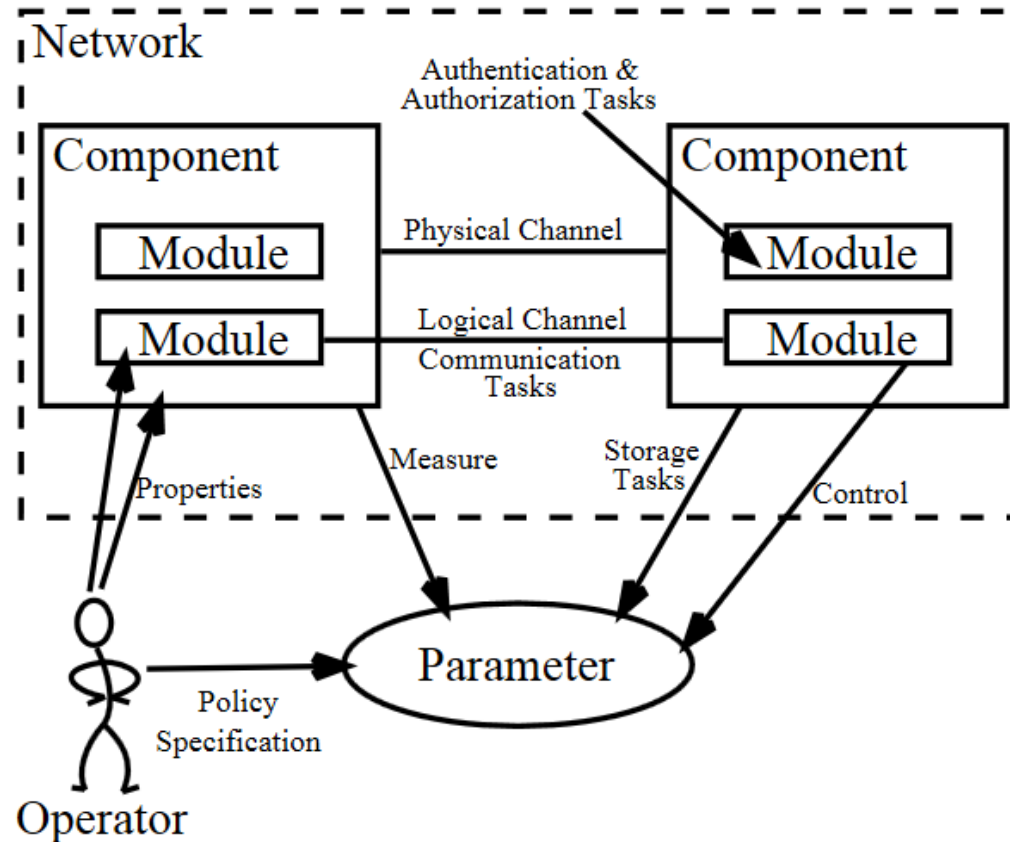


IDP 3

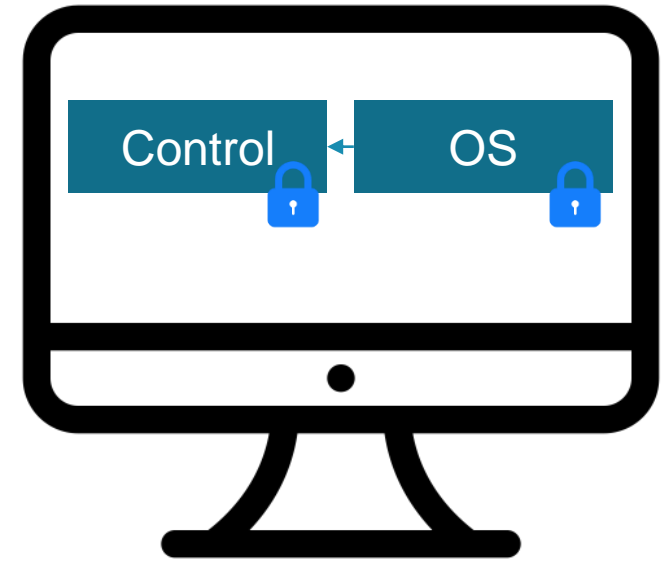
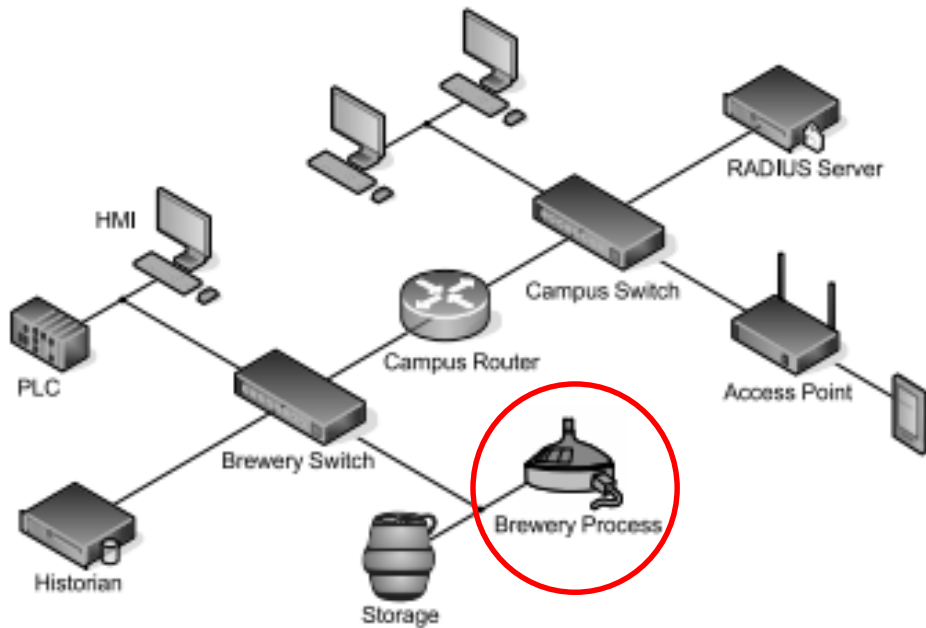


- Imperative Declarative Programming framework
- Extension of first order logic
 - Inductive definitions
 - Aggregates
 - Partial functions
 - ...
- IDP instance consists of:
 - Vocabulary
 - Theory
 - Structure
- Solves search problems using model expansion

Model - Conceptual



Model - Example



ICS-CERT

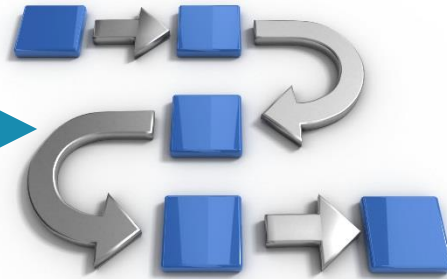


ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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

Feedback



Component vulnerabilities
ICS CSR 2

System vulnerabilities
ICS CSR 3

Simulations
(JISA Journal)

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



Input Model

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

	$Temp_{S_1}$	$Alarm_{S_1}$	$Humidity_{S_2}$
<i>Technician</i>	<i>R</i>	<i>R M</i>	<i>R</i>
<i>Operator</i>	<i>R M</i>	<i>R M</i>	<i>R M</i>
<i>Manager</i>	<i>R M</i>	<i>R M</i>	<i>R M</i>
<i>Attacker</i>			

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

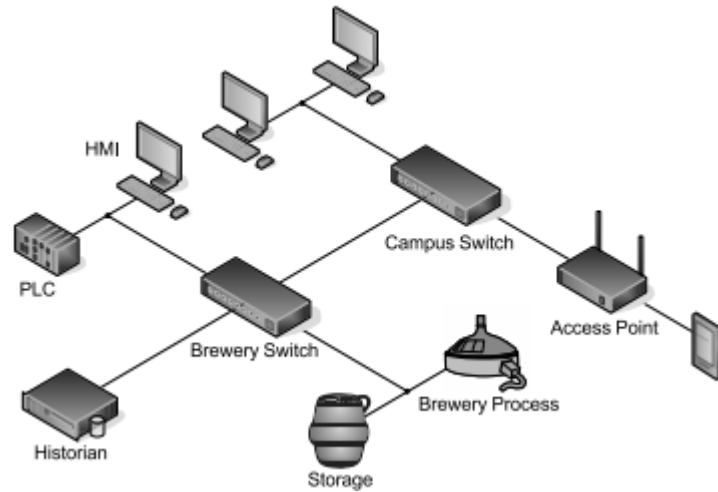
Case Study - Simulations

- Using our tool in the design phase of your system

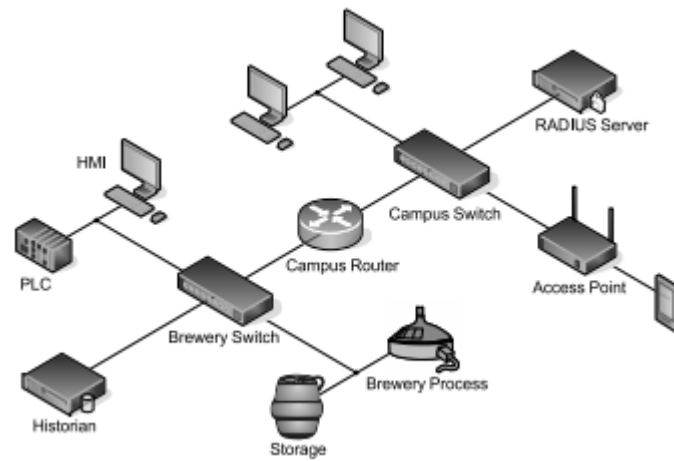


- Test different kinds of architectures
 - Simulate the effects of attacks or components failing
- Case study: brewery
 - Connect the brewery to the campus network
 - Three different architectures
 - Several simulations

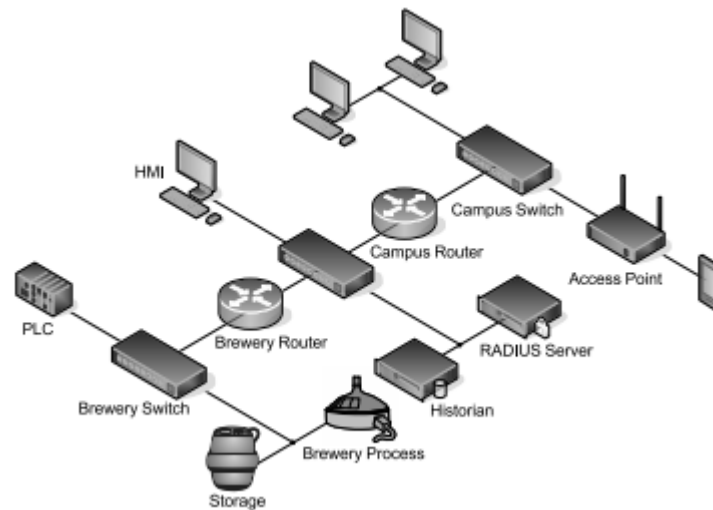
Architectures



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 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:  
((? 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
```

Conclusion

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

Questions?

