

**The European Commission's
science and knowledge service**

Joint Research Centre

Chemical Accident Risks Seminar

**Session 3 - Cybersecurity of Industrial
Control Systems: New technology challenges,
facts & constraints and Int'l policy context**

Marc HOHENADEL, PhD

15 June 2017



European
Commission

Risk level and impact of a cybersecurity incident



Business organisation

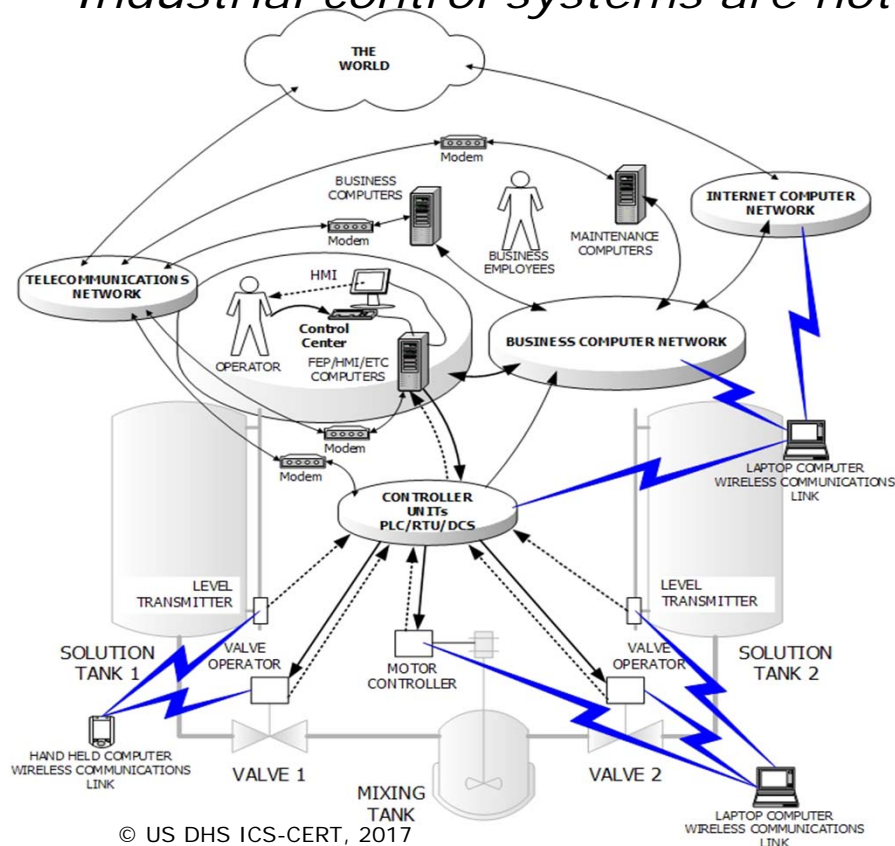
Business disruption
Lost of reputation
Leak of information

Industry

Environmental damages
Staff and public health
Societal impact

Newly technological challenges

Industrial control systems are not isolated anymore



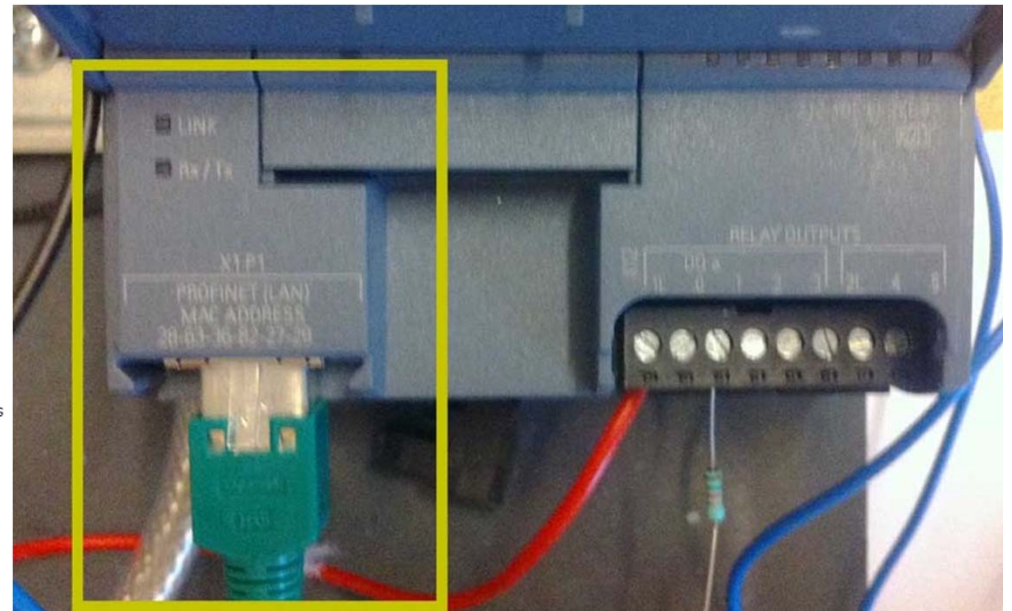
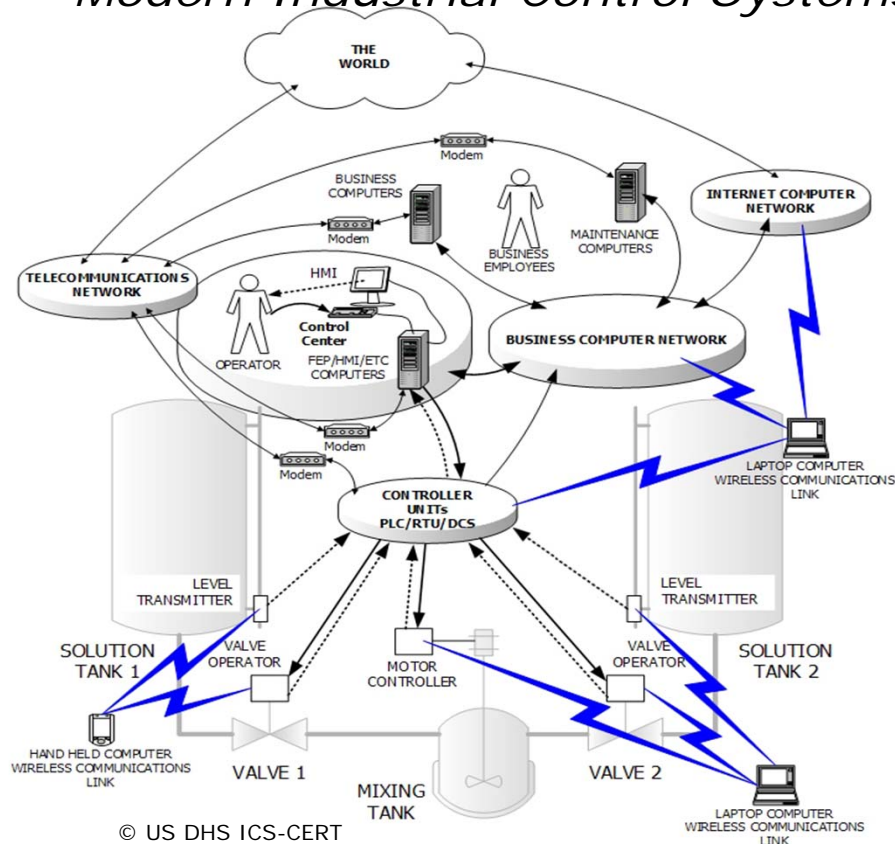
© Fortinet, Inc. , 2000-2017



European
Commission

Newly technological challenges

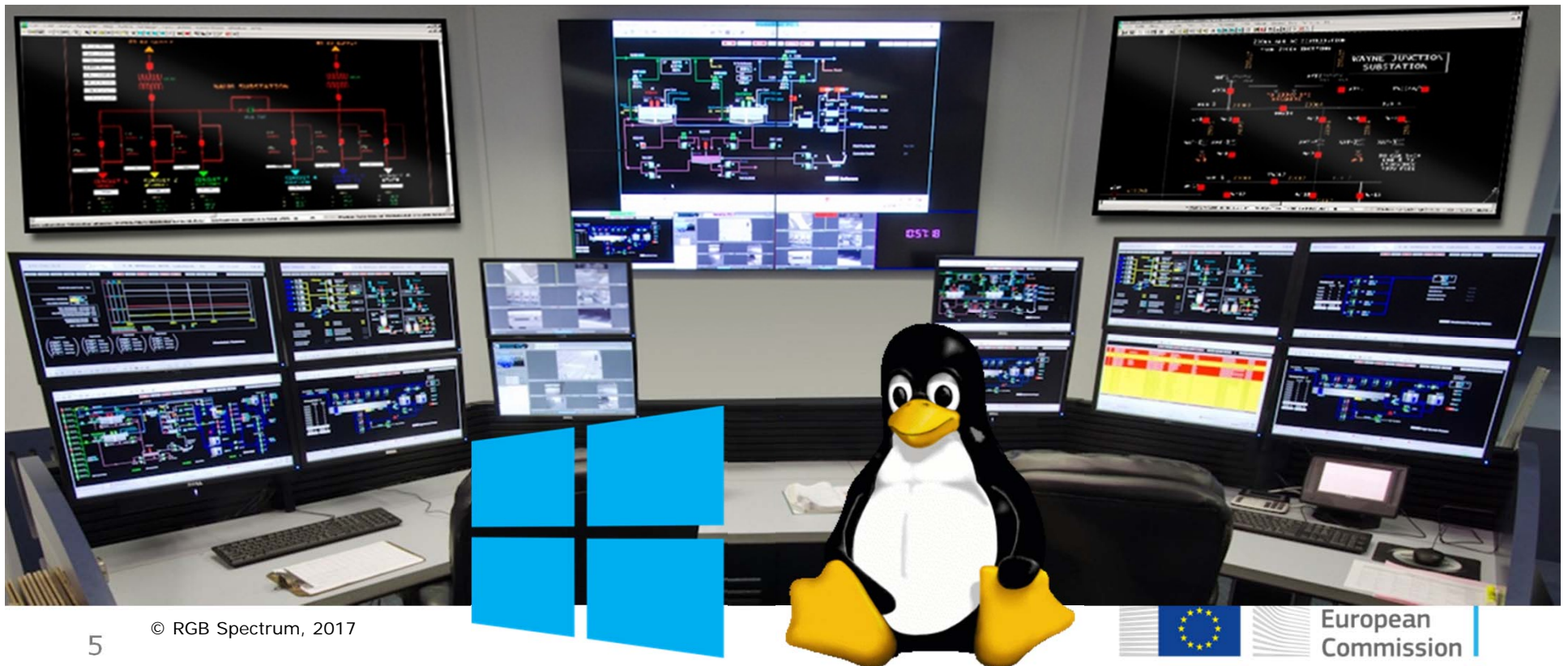
Modern Industrial Control Systems are communicating over TCP/IP



© PLC Academy, 2015

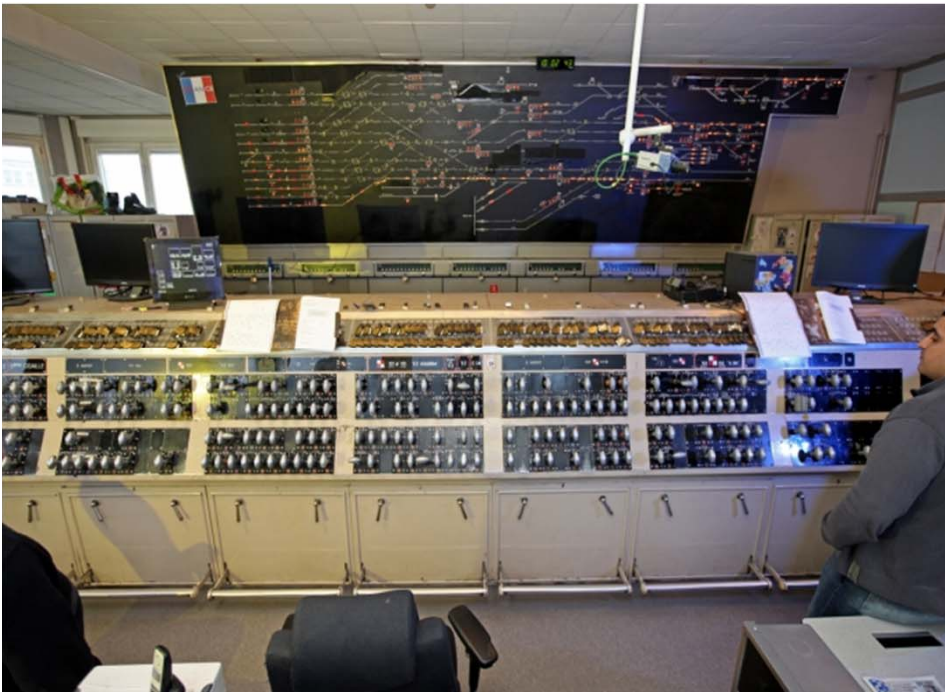
Newly technological challenges

Industrial Control Systems are running generic OS



Facts & constraints

Support legacy systems, lifetime of components



© SNCF, 2017



European
Commission

Facts & constraints

Patching industrial control systems is pain!



© Rousselet Robatel, 2017

Facts & constraints

Lack of awareness



The screenshot shows the ICS-CERT website with a search bar at the top. The main content area displays an advisory titled "Advisory (ICSA-16-075-01) Siemens SIMATIC S7-1200 CPU Protection Mechanism Failure". The advisory text states that Siemens has identified a protection mechanism failure vulnerability in old firmware versions of SIMATIC S7-1200. It mentions that the Department of Homeland Security (DHS) does not provide any warranties and that further dissemination is governed by the Traffic Light Protocol (TLP) marking. A sidebar on the left contains links to various sections like Control Systems, Home, Calendar, ICSJWG, Information Products, Training, Recommended Practices, Assessments, Standards & References, Related Sites, and FAQ.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

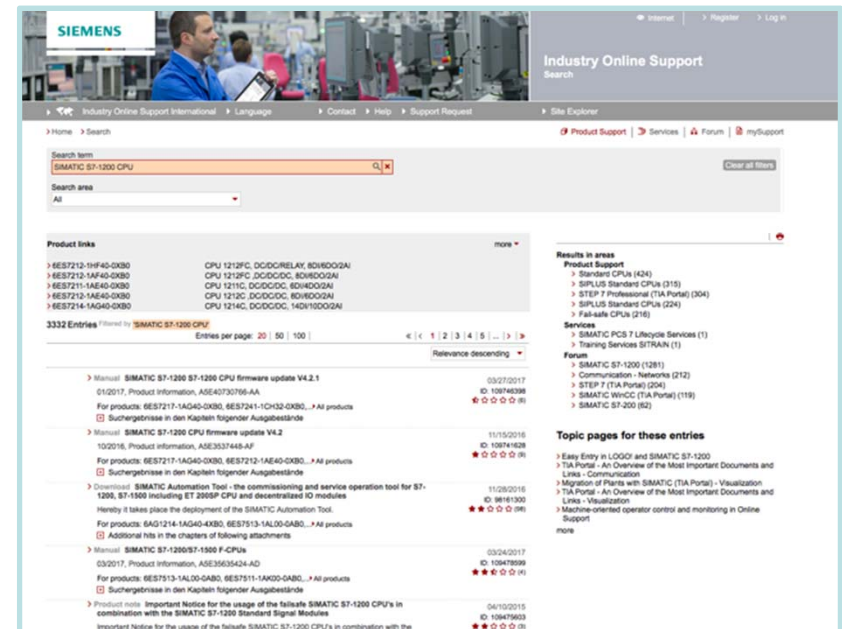
Advisory (ICSA-16-075-01)
Siemens SIMATIC S7-1200 CPU Protection Mechanism Failure
Original release date: March 15, 2016

Legal Notice
All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

OVERVIEW
Siemens has identified a protection mechanism failure vulnerability in old firmware versions of SIMATIC S7-1200. Maik Brüggemann and Ralf Spennenberg from Open Source Training reported this issue directly to Siemens. Siemens provides SIMATIC S7-1200 CPU product, release V4.0 or newer, to mitigate this vulnerability and recommends keeping the firmware up to date.

This vulnerability could be exploited remotely.

© US DHS ICS-CERT, 2017



The screenshot shows the Siemens Industry Online Support website. A search bar at the top contains the text "SIMATIC S7-1200 CPU". Below the search bar, there are several search results listed, including product links, manuals, and important notices. The results are sorted by relevance, and the first result is "SIMATIC S7-1200 CPU firmware update V4.2.1".

Siemens
Industry Online Support

Search term: SIMATIC S7-1200 CPU
Search area: All

Product links
more
6ES7212-1BH40-0XB0 CPU 1212C, DC/DC/RELAY, 80I/8DO/2AI
6ES7212-1BH40-0XB0 CPU 1212C, DC/DC/DC, 80I/8DO/2AI
6ES7212-1BH40-0XB0 CPU 1212C, DC/DC/DC, 80I/8DO/2AI
6ES7212-1BH40-0XB0 CPU 1212C, DC/DC/DC, 80I/8DO/2AI
6ES7212-1BH40-0XB0 CPU 1212C, DC/DC/DC, 80I/8DO/2AI

3332 Entries Filtered by SIMATIC S7-1200 CPU
Entries per page: 20 | 50 | 100 | < | 1 | 2 | 3 | 4 | 5 | > |

Relevance descending

Results in area:
Product Support
Standard CPUs (140)
SIPUS Standard CPUs (315)
STEP 7 Professional (TIA Portal) (304)
SIPUS Standard CPUs (224)
Fail-safe CPUs (216)
Services
SIMATIC PCS 7 Lifecycle Services (1)
Training Services SITRAIN (1)
Forum
SIMATIC S7-1200 (1281)
Communication - Networks (212)
STEP 7 (TIA Portal) (204)
SIMATIC HWCC (TIA Portal) (118)
SIMATIC S7-200 (82)

Topic pages for these entries
Easy Entry in LOGO! and SIMATIC S7-1200
TIA Portal - An Overview of the Most Important Documents and Links - Communication
Migration of Plants with SIMATIC (TIA Portal) - Visualization
TIA Portal - An Overview of the Most Important Documents and Links - Visualization
Machine-oriented operator control and monitoring in Online Support
more

© Siemens AG, 2017

International policy context

ENISA, the EU agency for Network and Information Security

The screenshot displays the ENISA website interface. At the top, the ENISA logo and name are visible, along with the European Union flag and navigation links for TOPICS, NEWS, PUBLICATIONS, and EVENTS. A search bar and a language selector (set to English) are also present. Below the navigation bar, a breadcrumb trail indicates the current page: Home > Publications > Protecting Industrial Control Systems. Recommendations for Europe and Member States.

Topic

- ^ Critical Infrastructures and Services
 - > ICS SCADA

Keywords

- Resilience

Protecting Industrial Control Systems. Recommendations for Europe and Member States

The report describes the current situation of Industrial Control Systems security and proposes seven recommendations to improve it. The recommendations call for the creation of the national and pan-European ICS security strategies, the development of a Good Practices Guide on the ICS security, fostering awareness and education as well as research activities or the establishment of a common test bed and ICS-computer emergency response capabilities.

Published December 14, 2011
Language English

Download
PDF document, 1.44 MB

Recommended publications

Communication network dependencies for ICS/SCADA Systems

ENISA is continuing the work on communication network dependencies in industrial infrastructures, focusing in this case on ICS/SCADA systems and...

Published on February 01, 2017

Analysis of ICS-SCADA Cyber Security Maturity Levels in...

Published on December 11, 2015

Certification of Cyber Security skills of ICS/SCADA...

Published on February 19, 2015

Good Practices for an EU ICS Testing Coordination Capability

© ENISA, 2017

International policy context

US NIST, Special Publication (NIST SP) - 800-82 Rev 2

NISTSearch NISTNIST MENU

NEWS

NIST Releases Update of Industrial Control Systems Security Guide

June 05, 2015

The National Institute of Standards and Technology (NIST) has issued the second revision to its [Guide to Industrial Control Systems \(ICS\) Security](#). It includes new guidance on how to tailor traditional IT security controls to accommodate unique ICS performance, reliability and safety requirements, as well as updates to sections on threats and vulnerabilities, risk management, recommended practices, security architectures and security capabilities and tools.

Downloaded more than 3 million times since its initial release in 2006, the ICS security guide advises on how to reduce the vulnerability of computer-controlled industrial systems to malicious attacks, equipment failures, errors, inadequate malware protection and other threats.



Credit: ©Microvector/Shutterstock

Share

f

g+

tw

ORGANIZATIONS

Engineering Laboratory
Intelligent Systems Division

RELATED CONTENT

[NIST Seeks Comments on Major Revision to Industrial Control Systems Security Guide](#)

[NIST Releases Update of Industrial Control Systems Security Guide for Final Public Review](#)

[EL Highlights May 2014](#)

© ENISA, 2017

International policy context

Directive (EU) 2016/1148 of 6 July 2016



Stay in touch



EU Science Hub: [*ec.europa.eu/jrc*](https://ec.europa.eu/jrc)



Twitter: [*@EU_ScienceHub*](https://twitter.com/EU_ScienceHub)



Facebook: [*EU Science Hub - Joint Research Centre*](https://www.facebook.com/EU_Science_Hub_-_Joint_Research_Centre)



LinkedIn: [*Joint Research Centre*](https://www.linkedin.com/company/joint-research-centre)



YouTube: [*EU Science Hub*](https://www.youtube.com/EU_Science_Hub)