JPCERT CC®

制御システム・セキュリティの現在と展望

Status and Prospects on ICS Security

この1年間を振り返って

Looking back over this one year

2014年2月5日
JPCERTコーディネーションセンター
理事・顧問　宮地　利雄

概要

Summary of Look-backs

1. ICS製品の脆弱性
   - 発見された脆弱性
   - 脆弱性の取扱
2. ICS上のサイバー・インシデント
   - ニュースになったICSインシデント
   - 重要インフラ事業者を狙う標的型攻撃
   - マルウェア感染
   - インターネットに直結されたICS
3. ICSセキュリティ関連の標準
   - 標準規格
   - 認証制度
4. ICSセキュリティ関連の研究開発活動

1. Vulnerabilities on ICS products
   - Reported vulnerabilities
   - Processes and framework for handling vulnerabilities
2. Cyber incidents on ICS
   - Incidents reported on news media
   - Targeted attacks against critical infrastructure providers
   - Malware infection on ICS
   - Internet reachable ICS
3. Standards on ICS security
   - Standards
   - Certifications
4. Research and development on ICS security

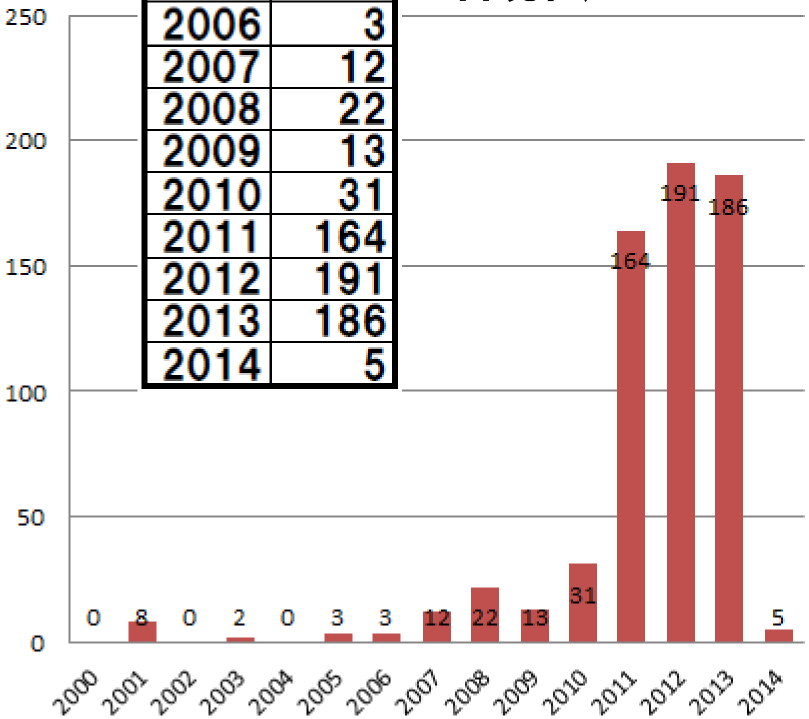
制御システム製品の脆弱性

Vulnerabilities in ICS products

- **脆弱性の報告数の高止まり**
  Number of vulnerability reports remains high.
  - **伸びは一服**
    No more rocket upsurge, but at a high altitude
- **DNP3に関連する脆弱性の衝撃**
  Shockwave of vulnerabilities found in DNP3 products
  - **脆弱性探索技術の高度化**
    Sophistication of fuzzing techniques
- **脆弱性の取扱制度の動向**
  Trends on vulnerability handling
  - **国際標準**
    International standard
  - **国内制度の検討**
    Framework in Japan
  - **ベンダーによる報奨金**
    Bounty program by vendors

OSVDBに登録された制御システム製品の脆弱性件数
(2014年1月19日現在)

年	件数
2000	0
2001	8
2002	0
2003	2
2004	0
2005	3
2006	3
2007	12
2008	22
2009	13
2010	31
2011	164
2012	191
2013	186
2014	5

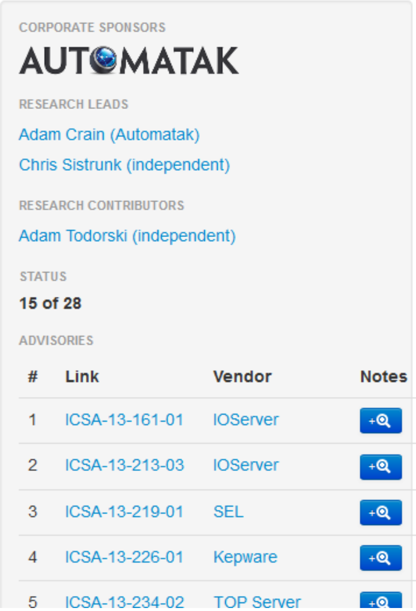


DNP3製品の脆弱性の余波

Shockwave of vulnerabilities in DNP3 products

- Adam Crain氏が9月13日に公表
  Mr. Adam Crain disclosed them on September 13
  - 開発中のDNP3ファザーを2014年3月に公表予定
    He said that he was developing a fuzzing tool for DNP3 and that he would release it in March, 2014
    - Modbus, IEC 61850, ICCP/TASE.2も計画中 (in their future plan)
  - DNP3製品の脆弱性を多数発見しICS-CERTに報告中
    He had found a number of vulnerabilities on various DNP3 implementations and reported them to ICS-CERT

Aegis Platform



CORPORATE SPONSORS

AUTOMATAK

RESEARCH LEADS

Adam Crain (Automatak)

Chris Sistrunk (independent)

RESEARCH CONTRIBUTORS

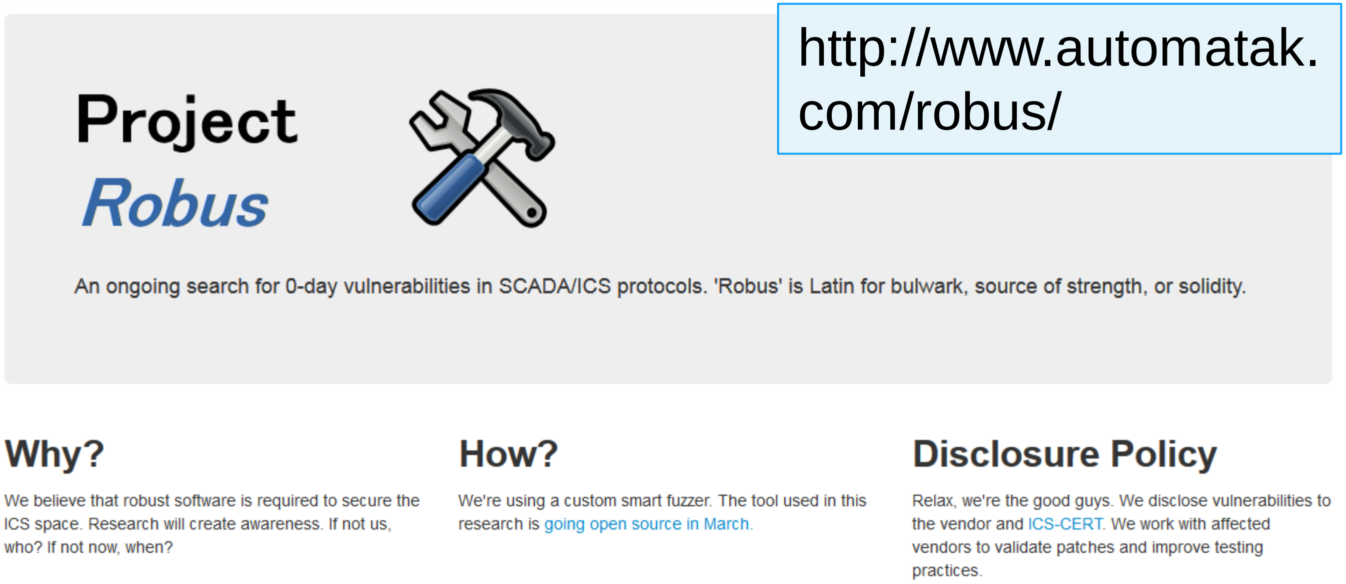
Adam Todorski (independent)

STATUS

15 of 28

ADVISORIES

#	Link	Vendor	Notes
1	ICSA-13-161-01	IOServer	+🔍
2	ICSA-13-213-03	IOServer	+🔍
3	ICSA-13-219-01	SEL	+🔍
4	ICSA-13-226-01	Kepware	+🔍
5	ICSA-13-234-02	TOP Server	+🔍



http://www.automatak.com/robus/

Project *Robus*

An ongoing search for 0-day vulnerabilities in SCADA/ICS protocols. 'Robus' is Latin for bulwark, source of strength, or solidity.

Why?

We believe that robust software is required to secure the ICS space. Research will create awareness. If not us, who? If not now, when?

How?

We're using a custom smart fuzzer. The tool used in this research is going open source in March.

Disclosure Policy

Relax, we're the good guys. We disclose vulnerabilities to the vendor and ICS-CERT. We work with affected vendors to validate patches and improve testing practices.

DNP3とは？

What is DNP3?

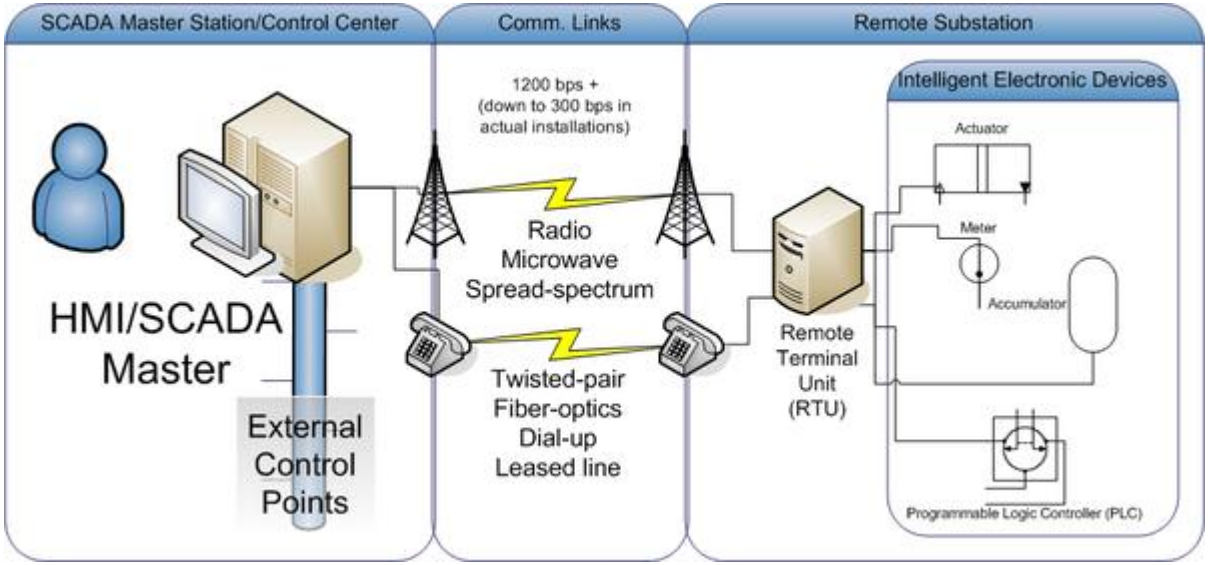
Distributed Network Protocol

- HMI/SCADA～RTU間で利用される通信プロトコル

  Communication protocol used between HMI/SCADA and RTU
- 電力と水道業界でもっぱら利用

  Mainly used in electric companies and water companies
- 日本では馴染みが薄いが，米国等で広く利用されている

  Widely used in the U.S. and other countries although not so popular in Japan



出典: WikiPedia

DNP3の脆弱性で注目される点

What is unique about the DNP3 vulnerabilities?

- ICSプロトコルに対する初の体系的なファジング
  First systematic fuzzing on an ICS protocol
  - EDSAのファジング試験(通信耐性試験)では
    イーサネットやTCP/IPだけが対象
    Current fuzzing test of EDSA certification (CRT: Communication Robustness Test) covers only Ethernet and basic TCP/IP protocols
  - DNP3以外のICSプロトコルの実現も同程度に脆弱か
    Implementation of other ICS protocols seems to be as vulnerable as DNP3's

- シリアル回線からも攻撃が可能
  The vulnerabilities can also be exploited through serial communication lines.

- PLC/RTU側だけでなくHMI/SCADA側の脆弱性も探索
  Fuzzing not only on the PLC/RTU side but also on the HMI/SCADA side

DNP3の脆弱性が意味するもの

What DNP3 vulnerabilities mean

- ICSプロトコルは堅牢だとの神話も崩壊

  Some Japanese ICS experts said that ICS protocols are implemented robustly but it is only a dream

  - 従来はICSプロトコル用の試験ツールが未整備なために発見される脆弱性が少なかったに過ぎない

    The number of vulnerability reports on ICS protocols was low so far, just because fuzzing test has been applied to them rarely.

  - ICSプロトコル・スタックに潜在する脆弱性がツールが整備されるにつれて発見されそう

    Vulnerabilities on ICS protocols will be often reported as test tools become widely used in the future.

- センター側の方が末端側よりも攻撃の打撃が広域に及ぶ

  Exploitation against the center side equipment is more attractive than the terminal side for attackers.

  - 末端が広域に分散しているシステムにおいては物理的な防御が困難

  - 遠隔の端末の位置からセンター側が攻撃される可能性

HARTプロトコルの脆弱性

(Highway Addressable Remote Transducer)

- 多くの先進的フィールド機器に，監視システムとの情報交換のために実装されたプロトコル

  HART protocol is the standard for sending and receiving digital information between smart devices and control or monitoring system.
  http://www.hartcomm.org/protocol/about/aboutprotocol_what.html

- Ralph Langner氏他のICSセキュリティ専門家が深刻な被害につながる可能性がある脆弱性がHARTプロトコルに存在することを報告

  Ralph Langner and other ICS cyber security experts have warned that the critical ICS vulnerabilities that can cause significant damage and/or personal injuries lie in the functional design of the instrumentation and control systems.
  http://www.controlglobal.com/blogs/unfettered/an-ics-cyber-vulnerability-beyond-stuxnet/

脆弱性取扱の手順のガイドライン制定

Guidelines on vulnerability handling processes

- 脆弱性のベンダーによる取扱に関する国際標準の制定

  International standardization on how vendors should handle vulnerability reports

  - ISO/IEC 30111 (脆弱性取扱手順)：国際標準として11月1日発行

    "Vulnerability handling processes" was published as an international standard.
  - ISO/IEC 29147 (脆弱性開示)：国際標準として承認

    "Vulnerability disclosure" was approved as an international standard.

- 2004年から運用されてきた国内の脆弱性届出制度をICS分野に拡大することを検討中
  - The vulnerability handling program coordinated by IPA and JPCERT/CC has been operated in Japan since 2004.
  - Its extension to ICS products has been studied in the vulnerability research committee convened by IPA.

脆弱性報告の報奨制度と闇市場

Bounty programs and black markets for bugs and vulnerabilities

- バグ報奨金制度はベンダーにとってうまみ (CMU研究者)

  CMU researchers said that bug bounty program may be beneficial for vendors.
  http://www.networkworld.com/news/2013/071013-study-bug-bounty-programs-provide-271650.html

  - Microsoft, Google, Mozilla

- 制御システム・ベンダー(Integraxor社)も

  Integraxor became the first ICS vendor who started bug bounty program.
  http://www.integraxor.com/blog/integraxor-hmi-scada-bug-bounty-program/

  - 製品の利用権を報奨として提供

- ロシアのサイバー犯罪市場が2012年に19億ドル規模に(グループIB社の見積り)

  Group IB estimated that Russian cyber crime market had expanded to 1.9 billion dollar size in 2012.
  http://www.securityweek.com/russia-cybercrime-market-reached-19-billion-2012-group-ib-estimates

セキュリティ・インシデントの動向

Trends on cyber security incidents

- 深刻なサイバー攻撃の報告は無かった

  No ICS security incident affecting widely and severely has been reported.

- 研究発表としてのICS攻撃デモ

  A lot of attack techniques against ICS have been demonstrated and reported in various technical conferences.

- 重要インフラ事業者へのAPTが深刻化ないし高水準維持

  APT continues to be in a severe level or worsens at critical infrastructure service providers.

- CSのマルウェア感染がかなり広範囲に散発

  Malware infection of ICS seems to have occurred more often than expected.

- インターネットに直結された制御システムも減らず

  Many ICSs or ICS products have been found on the Internet.

深刻なサイバー攻撃の報告は無い

No critical cyber security incident on ICS is reported

- ハッカー団「シリア電子軍」がイスラエルのICSを攻撃

  A attacker group called “Syrian Electric Army” breached an ICS in Israel.
  http://abna.ir/data.asp?lang=3&Id=417250
  http://news.softpedia.com/news/Syrian-Electronic-Army-Claims-to-Have-Hacked-Israeli-Critical-Infrastructure-Systems-351779.shtml

  - 「イスラエルの重要インフラに侵入」との犯行声明だった

    They declared that they have breach a critical infrastructure of Israel.

  - 侵入したICSは農業灌漑ポンプだった模様

    The ICS is for an irrigation system of a small farm.

- イスラエルの道路トンネル管理システムにサイバー攻撃

  A cyber attack on a tunnel in Israel was reported.
  http://phys.org/news/2013-10-israeli-tunnel-cyber.html

  - 保安用カメラを狙ったトロイの木馬による攻撃

    Trojan horse attack targeted the security camera system

  - 9月8日に20分間，9月9日に8時間にわたり通行止め

    The roadway was shut down for 20 minutes on September 8 and for 8 hours on September 9

標的型サイバー攻撃とICS

Targeted cyber
attack and ISC

- 重要インフラ事業者への標的型サイバー攻撃の深刻化に米国DHSが懸念

  U.S. DHS alerted that critical targeted cyber attacks on critical infrastructure providers operating their ICSs had been often observed.
  http://www.securityweek.com/dhs-spear-phishing-campaign-targeted-11-energy-sector-firms

  - サイバー攻撃がICSに及んだ事例は極めて少ないが，
    社内情報システム内でICS関連情報を探し回った形跡
  - 標的になっているのはエネルギー業界

    Especially, providers of the energy industry.

- 中小を含む製造事業者にも多数(24%)の標的型サイバー攻撃
  (Symantec社が報告)

  Symantec reported that manufacturers including MSB was most common targets of cyber attacks.
  http://www.symantec.com/security_response/publications/threatreport.jsp?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Apr_worldwide_ISTR18

緊張する朝鮮半島

International tension mounted
in the Korean Peninsula

- 北朝鮮からのサイバー攻撃を韓国政府が発表

  South Korean government alerted about cyber attacks by North Korea.

- 韓国が原子力発電所のICS網でセキュリティ対策

  S. Korea divides nuclear plant controls from Internet (4月14日)

  http://english.yonhapnews.co.kr/business/2013/04/14/65/0503000000AEN20130414000500320F.HTML

  - ICS網をイントラネットおよびインターネットから完全に分離

    ICS networks on nuclear plants were separated completely from intranets and the Internet.

ICSに対する攻撃に関する研究発表

Research reports on attack against ICSs

- ビル制御システム (2月6日)

  Researchers Demo Building Control System Hack
  http://www.darkreading.com/security/vulnerabilities/240147983/researchers-demo-building-control-system-hack.html

- ビル暖房システムに脆弱性

  Security hole can damage heating systems
  http://www2.majorgeeks.com/story.php?id=38552

- 頻発していると見られるICS内でのマルウェア感染
  公式の統計情報がないが…

  Malware infection in ICS is often reported though there is no formal statistics.

  — あるウィルス対策製品ベンダーによれば
  ICSを利用している顧客企業の3割でマルウェア感染
  うち4割は操業の継続に影響

  According to an anti-virus vendor’s notice, 30% of their Japanese customers operating ICS have had their ICS infected by malware, 40% of which have been forced to discontinue their normal business operation.

インターネットに直結された制御システム

ICS reachable
from the Internet

- コンピュータ(インターネット・サーバ)検索サービスのShodan

  "Shodan" is a service for searching computers on the Internet.

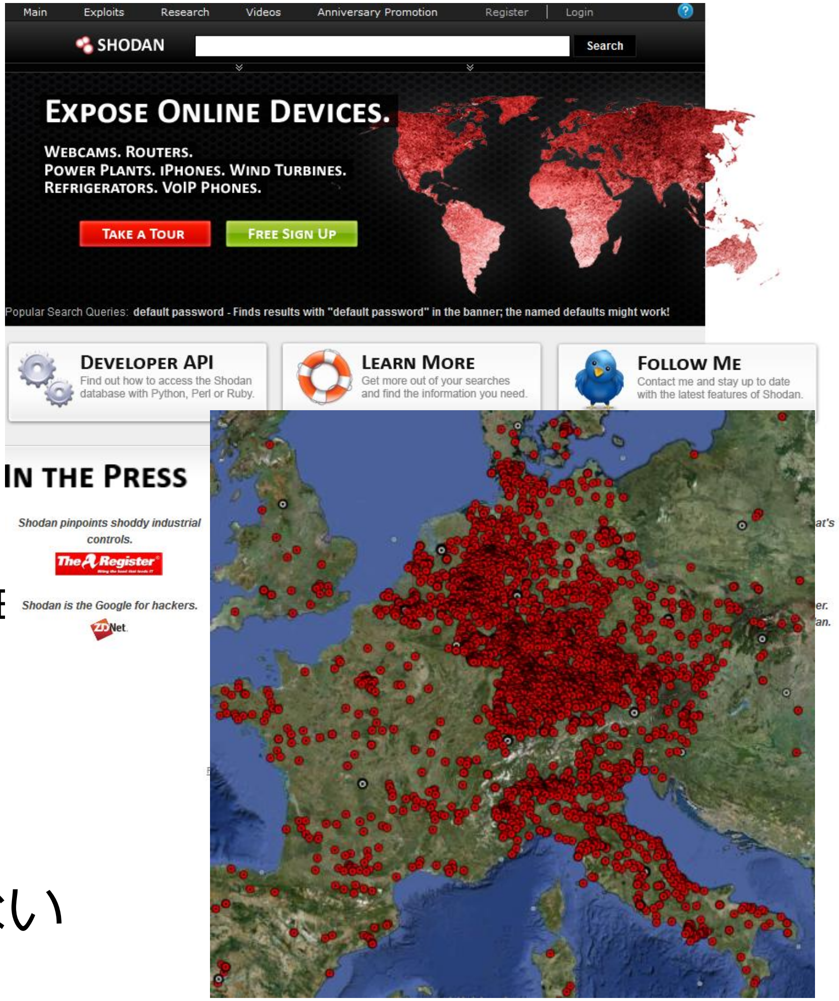
  http://www.shodanhq.com/

- 見えてきた検索キーワード

  Keywords for searching ICS have been shared in the researchers' community.

  —SHINEプロジェクト等で数十万台規模の製品を発見

  About a million ICS products have been identified by several projects such as SHINE



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

Shodan pinpoints shoddy industrial controls.

Shodan is the Google for hackers.

- 減らない

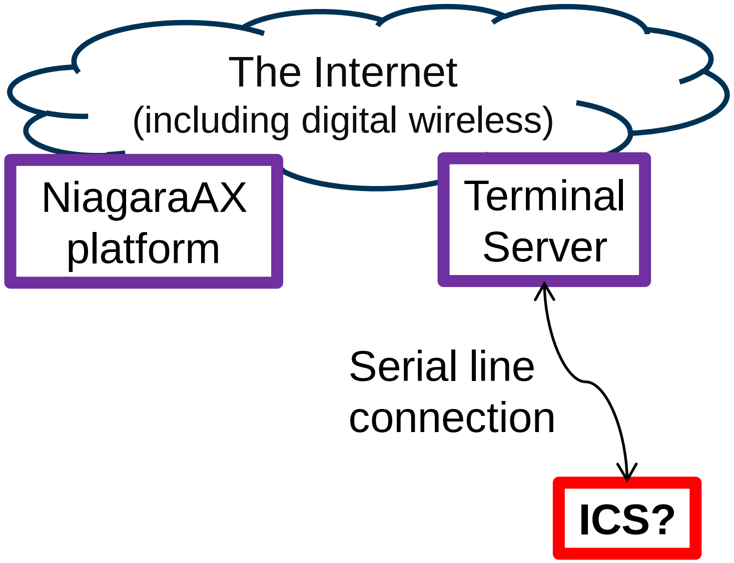
  Japanese cases is not so many but still remain.

  —日本の事例はそれほど多くはない

インターネット直結の制御システム事例

Cases of Internet reachable ICS

- 特定のビル制御用ICS製品(Cylance社が報告)
  http://www.computerworld.com/s/article/9239040/Researchers_find_hundreds_of_insecure_building_control_systems
- インターネットに接続された多数(11.4万台)のターミナル(シリアル回線)サーバー (Rapid7社が報告)
  Rapid7 reported 114 thousand terminal servers were reachable via the Internet.
  https://community.rapid7.com/servlet/JiveServlet/downloadBody/2271-102-1-4509/Serial%20Offenders%20FAQ.pdf
  https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers
  - シリアル回線で接続されている機器の多数がレガシーICS？



Terminal servers

ICSハニーポットによる調査

Research with ICS honeypot

- TrendMicro社がICSに見せかけたハニーポットを設置し攻撃活動を調査報告

  TrendMicro installed multiple ICS honeypots and investigated activities attacking them.

  — Who’s Really Attacking Your ICS Equipment?
    http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf

  — The SCADA That Didn’t Cry Wolf
    https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf

- HoneyNetプロジェクトがConPot (Control Honeypot)を公表

  HoneyNet Project released Control Honeypot or ConPot for short, which simulated ICSs including Siemens SIMATIC S7-200 PLC.
  http://www.honeynet.org/node/1047

  — Siemens SIMATIC S7-200 PLC等をソフトウェアで模擬

- 油井施設に見せかけたハニーポットに侵入

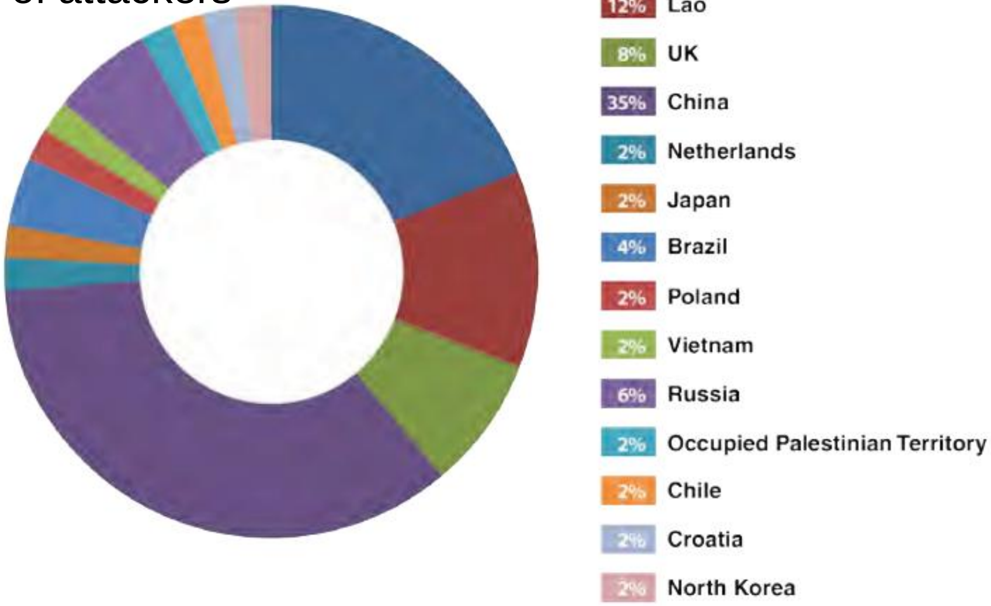
  Cyber attacks were observed on a honeypot simulating a oil rig.
  http://www.theregister.co.uk/2013/08/01/scada_plc_vulnerability/

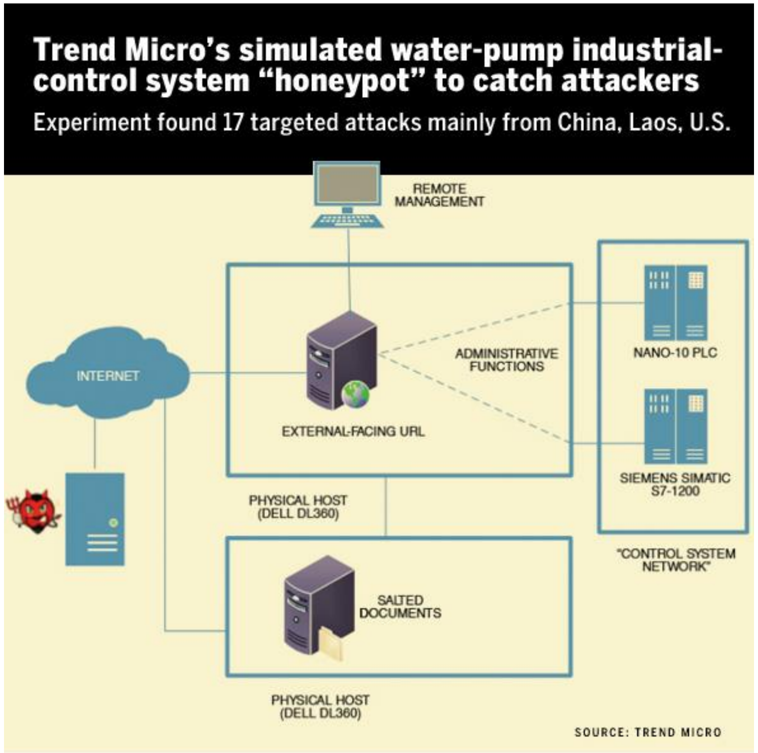
TrendMicro社のICSハニーポット

ICS honeypot operated by TrendMicro

- TrendMicro社の研究者がICSハニーポットを インターネット上に構築して攻撃の様子を観測
  http://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/
  http://blog.trendmicro.co.jp/archives/7740

Network location of attackers




Trend Micro's simulated water-pump industrial-control system "honeypot" to catch attackers

Experiment found 17 targeted attacks mainly from China, Laos, U.S.

SOURCE: TREND MICRO

サイバー・セキュリティ・インシデント訓練

Cyber Security
Incident Drills

- 国内初の電力・ガス・ビル分野のサイバー・セキュリティ演習実施 (経済産業省 ; 2013年2月4日)

  ICS cyber Security Incident Response Drills were carried out in electric, gas and building automation industries.
  http://www.meti.go.jp/press/2012/02/20130204002/20130204002.html
  http://www.arcweb.com/industry-news/2013-03-22/first-cyber-security-drills-conducted-in-electricity-gas-and-buildings-areas-in-japan.aspx

- 米国DoEの資金でNESCORが
  サイバー・セキュリティ事故シナリオと影響を分析

  The National Electric Sector Cybersecurity Organization Resource has published three cyber security failure scenario and impact analyses documents for the electric sector.
  http://www.smartgridnews.com/artman/publish/Technologies_Security/Here-s-exactly-how-a-cyberattack-will-bring-down-your-utility-6108.html

- 米国NERCが電力基幹網に模擬サイバー攻撃 (11月13日)

  GridEx II

  The North American Electric Reliability Council (NERC)
  launched a simulated attack on the U.S. power grid.
  http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html

Stuxnetその後

Sequel of Stuxnet

- Symantec社の研究者がStuxnet 0.5版を報告

  Revealed: Stuxnet “beta’s” devious alternate attack on Iran nuke program
  http://arstechnica.com/security/2013/02/new-version-of-stuxnet-sheds-light-on-iran-targeting-cyberweapon/
  http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

- 総括報告
  - Ralf Langner氏の最終Stuxnet分析報告書

    Final Stuxnet analysis by Mr. Ralf Langer
    http://www.langner.com/en/2013/11/20/langner%E2%80%99s-final-stuxnet-analysis-comes-with-surprises/
  - Stuxnetの本当の話 (The Real Story of Stuxnet)

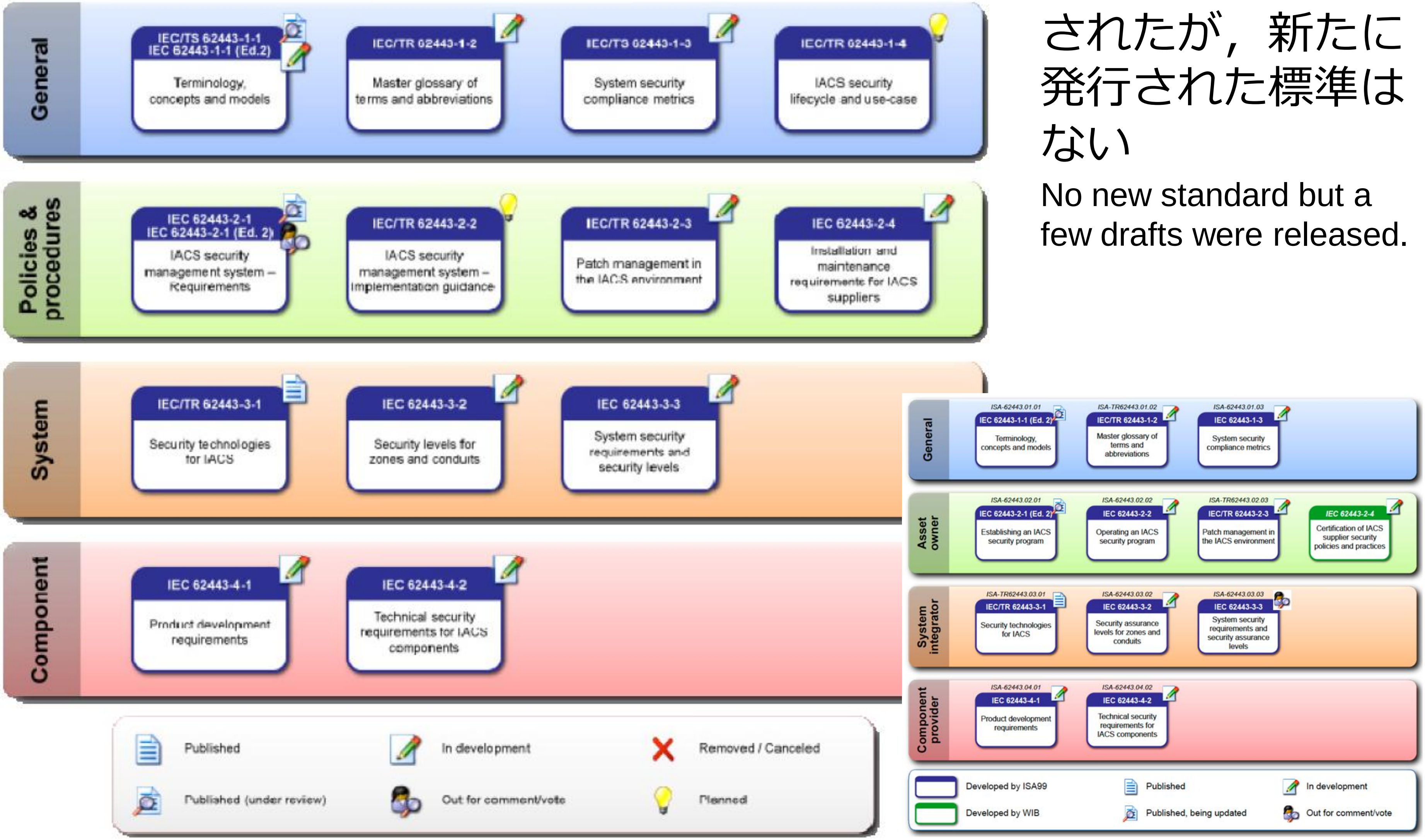
    http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

IEC 62443 (ISA-62443)シリーズ

http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx

複数の草案が公表されたが，新たに発行された標準はない

No new standard but a few drafts were released.



General
IEC/TS 62443-1-1
IEC 62443-1-1 (Ed.2)
Terminology, concepts and models
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
IEC/TS 62443-1-3
System security compliance metrics
IEC/TR 62443-1-4
IACS security lifecycle and use-case
Policies & procedures
IEC 62443-2-1
IEC 62443-2-1 (Ed. 2)
IACS security management system – Requirements
IEC/TR 62443-2-2
IACS security management system – Implementation guidance
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Installation and maintenance requirements for IACS suppliers
System
IEC/TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security levels for zones and conduits
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Product development requirements
IEC 62443-4-2
Technical security requirements for IACS components
Published
In development
Removed / Canceled
Published (under review)
Out for comment/vote
Planned
General
ISA-62443.01.01
IEC 62443-1-1 (Ed. 2)
Terminology, concepts and models
ISA-TR62443.01.02
IEC/TR 62443-1-2
Master glossary of terms and abbreviations
ISA-62443.01.03
IEC 62443-1-3
System security compliance metrics
Asset owner
ISA-62443.02.01
IEC 62443-2-1 (Ed. 2)
Establishing an IACS security program
ISA-62443.02.02
IEC 62443-2-2
Operating an IACS security program
ISA-TR62443.02.03
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Certification of IACS supplier security policies and practices
System integrator
ISA-TR62443.03.01
IEC/TR 62443-3-1
Security technologies for IACS
ISA-62443.03.02
IEC 62443-3-2
Security assurance levels for zones and conduits
ISA-62443.03.03
IEC 62443-3-3
System security requirements and security assurance levels
Component provider
ISA-62443.04.01
IEC 62443-4-1
Product development requirements
ISA-62443.04.02
IEC 62443-4-2
Technical security requirements for IACS components
Developed by ISA99
Developed by WIB
Published
Published, being updated
In development
Out for comment/vote

IEC 62443 (ISA-62443)シリーズ関連の動き

Prospects on IEC and ISA 62443

- ISO/IEC 27000シリーズの見直し
  - 中核部分を再構成中
  - 業界ごとISMSの拡充
    - ISO/IEC TR 27019 (エネルギー業界のためのISMS)
    - IEC 62443もISO/IEC 270xxと二重採番標準をめざす

- ISAが62443-3-3を承認(8月)；62443-3-2の草案も公表

  Part 3-3: System Security Requirements and Security Levels
  http://www.isa.org/Template.cfm?Section=press_releases5&template=/ContentManagement/ContentDisplay.cfm&ContentID=94074
  Part 3-2: Security risk assessment and system design
  http://isa99.isa.org/Documents/Drafts/ISA-62443-3-2-WD.pdf

セキュリティ認証

Security certification

製品 Products	運用管理 Operation practice	人員 Staff’s skill
• EDSA (by ISASecure) • Achilles Communication Certification (by WurldTech)	• Achilles Practices Certification (by WurldTech) • CSMS (Control System Security Management System or AICSMS)	• GICSP (by SANSとICSベンダー) • ISASecure

EDSA (Embedded Device Security Assurance)

- ISASecureが認定
  Planned by ISASecure
- 製品の認証
  Product certification
  - 新しい認証：1
    まだ5製品のみ
    Only 5 products have been certified; One new certified product in a recent year

Look for the ISASecure^{TM} Compliant Registration Logo

Certified Device ISASecure

View List of Certified Devices >

ベンダー名	製品タイプ	モデル名
Honeywell Process Solutions	Safety Manager	HPS 1009077 C001
RTP Corporation	Safety manager	RTP 3000
Honeywell Process Solutions	DCS Controller	Experion C300
Honeywell Process Solutions	Fieldbus Controller	Experion FIM
横河電機 (Yokogawa)	Safety Manager	SCP451/461-11 ：Vnet/IP

- CSSCとIPAがISASecureと連携してEDSA認証の準備中
  CSSC and IPA are collaborating with ISASecure to kick off EDSA certification program in Japan

認証を受けたICS製品の数

製品認証	2010年	2014年
Achilles Communications Certification	22	135
MuDynamics	3	(Spirent社が買収) (acquired by Spirent)
ISA ISCI (EDSA)	0	5
Exida	1	

2010年時点の認証製品数はRagnar Schierholz氏らによる”Security Certification – A critical review”に依る

The number of certified products are based on a paper “Security Certification – A critical review” by Ragnar Schierholz et al.

ICSセキュリティ専門家の認定制度

- Global Industrial Cyber Security Professional (GICSP)
  http://www.prnewswire.com/news-releases/new-industrial-control-systems-cyber-security-certification-in-development-223462451.html
  - SANSの配下のGIAC(Global Information Assurance Certification)が主導
  - ABBやRockwell, Schneider, 横河などのICSベンダーやRedTiger, WurldtechなどのセキュリティテイTRIM会社や
    BP, Shellなど利用組織も参加

- ISAの専門家認定制度
  - Certified Control Systems Technician (CCST)
  - Certified Automation Professional (CAP)
  - 新たにCertified Mission-Critical Professional (CMCP)をノース・カロライナ州の5大学と開発
    http://www.automation.com/automation-news/industry/isa-to-develop-mission-critical-professional-certification-program

ICSセキュリティ研究施設(海外)

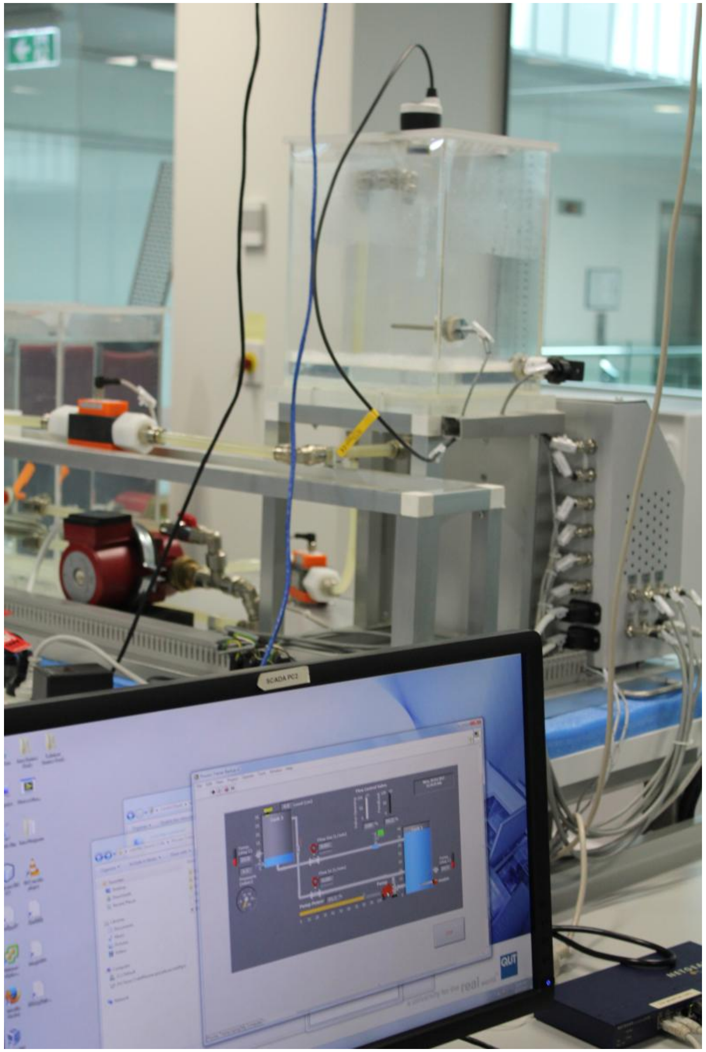
Research laboratories
for ICS security

- European Network for Cyber Security (ENSC)
  https://www.encs.eu/

- モントリオールにSCADAサンドボックス
  SCADA 'Sandbox' Tests Real-World Impact Of Cyberattacks On Critical Infrastructure in Montreal
  http://www.darkreading.com/taxonomy/index/printarticle/id/240149728

- スペインに産業用サイバー・セキュリティ・センター
  Spain to welcome the new Industrial Cybersecurity Center
  http://www.infosecurity-magazine.com/view/31095/spain-to-welcome-the-new-industrial-cybersecurity-center/

- 豪クイーンズランド工科大学 →
  Queensland University of Technology



ICSセキュリティ研究施設(日本)

Research laboratories for ICS security in Japan

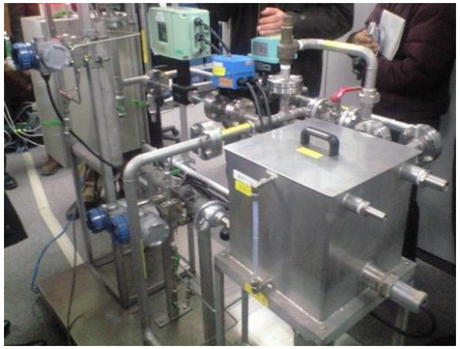
- 制御システムセキュリティセンター(CSSC)が東北多賀城本部を開設

  Control System Security Center or CSSC opened its Tohoku Tagajo headq

  http://www.css-center.or.jp/sympo/2013/documents/press20130513.pdf

- 名古屋工業大学の越島・橋本研究室

  —セキュリティ・デモ用のICS



- JPCERT/CCも技術的な検証環境を整備

御静聴ありがとうございました

Thank you for
your attention

ICSセキュリティは
世界規模の課題；
一朝一夕の解決は望めない；
10年単位の時間枠での取組を！

ICS security is a problem to be resolved globally;
There seems to be no simple solution;
Let’s resolve the problem in time range of a decade.