

Workshop on New Security Standards for IACS/SCADA Industrial Systems

Jan deMeer¹, Karl Waedt²

Abstract: The IACS/SCADA-Security WS aims at Security Standards and Practice for Industrial Systems integrated by a sort of Distributed Middleware I4.0. A short tutorial into Security Standards is given by the WS Co-Chairs. In-depth aspects of this issue is discussed and presented by the invited authors from China, UK and Germany presenting: IEC 62443 Security Standards - Humans, the strongest and weakest link - Integrity Monitoring - Policy-based Monitoring - 3D-Modelling - Graded Security Forensics etc.

Keywords: Reference Architecture Model for Industrie4.0 (RAMI), Middleware, Industrial Automation and Control Systems (IACS), Supervisory Control and Data Acquisition (SCADA) Systems, Security Standards and Techniques.

1 WS General Objectives

The expected multipart standard *IEC 62443-g-p*, or *ISA99* for 'Industrial Process Management and Control' comprises $g=4$ groups with $p \leq 4$ parts each group.

Group no.1 'General' contains the parts of the terminology used, glossaries, security compliance metrics and a part with use cases; Group no.2 'policy and procedures' contains parts of security management requirements, implementation guidance, patch management etc; group no.3 'system' contains parts of security technologies, security levels for zones and conduits, security level requirements; group no.4 'component' contains the parts of product development requirements, technical security requirements; the latter part **IEC62443-4-2** currently is under discussion by ISO/IEC experts and most probably will be published during 2016 which completes the IACS series.

Those standards find their considerations by '*Industrie4.0*' but also by SCADA system developments and security evaluations. That's the main objective of this workshop to discuss the relationships between

¹ smartspacelab.eu GmbH, Berner Str. 21B, 12205 Berlin, demeer@smartspacelab.de

² AREVA GmbH, PEAS-G, Henri-Dunant-Str. 50, 91058 Erlangen Karl.Waedt@areva.com

Industrial Standards addressing *IoT* vs. Industrial Systems implementing *IoT*³:



2 WS Participants Objectives

- to address the **Current Practice** of structuring, taking measures, evaluating benchmarking Industrie4.0 platforms and industrial automated control systems (IACS);
- to address Security Techniques, Architectures, Services, Features and Human-Machine-Interfaces in **Standardization** of Industrie4.0 platforms such as:
IEC TC65 Industrial Process Measurement, Control, Automation (IEC62443-p)
IEC TC57 Power System Management (IEC62351-p)
ISO JTC1/SC27 IT Security Techniques ISM, Process Control (ISO270 01/02/19)
BSI Protection Profile for Smart Grid GW, Energy Industry Act (TR03109)
ETSI CEN/CENELEC Smart Grid Coordination Group
NIST Smart Grid Interoperability Panel (NIST IR7628) etc.
- to address **Innovations** derived from features of industrial security & privacy standards and their impacts on industrial Control and Automation Systems IACS/SCADA/CRITIS;
- to address new Evaluation and Test Standards, i.e. '*Prüfnormen*', necessary to check correct implementations and impacts of **security & privacy measures in real and (ultra) large-scaled systems (ULS resp. CRITIS)**;
- to address **Laws and EU Regulations** that achieve Man-Machine Communication in the realm of 'Industrie4.0'.

³ Copyright of left picture is reserved by IACS/SCADA WS Programme Committee Members Rainer Falk, Steffen Fries Siemens München, Copyright of right picture is reserved by Jan deMeer, ssl.eu GmbH Berlin;

3 WS General Co-Chairs

Jan deMeer⁽¹⁾, Karl Waedt⁽²⁾

- 1) smartspacelab GmbH, AIT, Berner Str.21B, 12205 Berlin,
demeer@smartspacelab.de
- 2) AREVA GmbH, PEAS-G, Henri-Dunat-Str. 50, 91058 Erlangen,
Karl.Waedt@areva.com

4 WS Programme Committee Members

Scott Cadzow, C2 Ltd. UK, ETSI TC Cyber;

Rainer Falk, Siemens AG München, Corporate Technology;

Steffen Fries, Siemens AG München, Corporate Technology;

Gerard Gaudin, EU Club R2GS France;

Hans-Joachim Hof, MuSe Munich IT Security Research Group, Munich University of Applied Sciences;

Peter Schaar, EU Academy for Freedom of Information and Data Protection Berlin;

Maik Seewald, CISCO Systems München;

Ulrich Seldeslachts, EU Club R2GS Belgium;

Kristina Unverricht, DIN Consumer Council Berlin;

5 WS Programme Structure

The IACS/SCADA Industrial Security Workshop is organized as a **half-day workshop, 2016, Sept. 27, 9h00-12h30**, with 2 main sessions, each 90 minutes and a coffee break of 30 minutes; thus giving room to 3-4 workshop presentations per session, ca.20 minutes each and sufficient time for discussions even during coffee break.

The WS raises following questions and discusses answers:

1. Do we have good IEC Industrie4.0 Security Standard?

Jan deMeer, ssl.eu GmbH et al 'New Security Standards for Automation and Control Systems, based on IEC 62443-4-2 (IACS/SCADA)';

2. How can IAC/SCADA Systems be secured by ICT?

Scott & Alexander Cadzow, C2 Ltd. UK 'Humans - the strongest and weakest link

in Securing Systems';

Mithil Parekh, OvG University Magdeburg et al.: OPANSec - Security Integrity Monitoring for Controllers;

3. How can IACS/SCADA System Security be analyzed by Formal Models?

Yan Gao, OvG University Magdeburg et al. 'SIEM - Policy-based Monitoring of SCADA Systems';

Simon Seibt, TH Nuremberg Institute of Technology et al. '3D Modelling of Selected Assets, Security Zones and Conduits';

Jianghai Li, Tsinghua University Beijing, China: 'Graded Security Forensics Readiness of SCADA Systems';

An Overview about the WS Programme can be gained from the following outline

09:00	6 - Registration & Opening Session: What does Security mean to Industries? <i>Waedt, Karl, de Meer, Jan</i> 09:00 - 09:50	1 - New Industrial Security Standards for Industrial Automation and Control Systems, ... <i>Mr. Jan DE MEER et al.</i>
10:00	7 - How can IACS be secured by ICT? <i>Waedt, Karl</i> 09:50 - 10:45	0 - Humans - the weakest and strongest link in securing systems <i>Mr. Scott CADZOW et al.</i> 5 - OPANSec – Security Integrity Monitoring for Controllers <i>Mr. Mithil PAREKH</i>
	4 - Round Table Discussion with Hot Coffee	
11:00	2 - SIEM Framework for Policy-based Monitoring of SCADA Systems <i>Yuan GAO</i> 4 - 3D and 2D modeling of selected assets, security zones and security conduits <i>Mr. Simon SEIBT</i>	8 - How can IACS Security be analyzed by Models? <i>de Meer, Jan</i>
12:00	3 - Graded Security Forensics Readiness of SCADA Systems <i>Dr. Jianghai LI</i>	10:55 - 12:20
	5 - Wrap-up on Industrial Security WS	

6 WS Attendees Invited

- the IACS Workshop aims at practioners and engineers from Management, Administration, Security Operation, Security Incident Response Teams of SMEs and Providers of Industrial Infrastructures or Automated Control Systems;

- the IACS Workshop aims at experts from National, European and International Standardization & Regulation Alliances and Organizations such as DIN, ETSI, ISO/IEC, ANSSI, BSI, BNA, ENISA, CSA, ...
- the IACS Workshop aims at all Interested Parties, i.e. Students, Lecturers, Citizens of the Digital Society, who want to actively take part on the overwhelming industrial & societal revolution denominated as 'Industrie4.0' - Part-taking means to be a stakeholder (*Teilhaber*) and think about Regulations, Standards and IT-Laws on Privacy, Trustworthiness in Products, Built-in Security, Cyber Space Laws, Regulations and Measures to defend Cyber Crime

7 WS Background Information, Supporters and Links

<http://www.informatik2016.de/1127.html>

<http://germany.acm.org/aktivitaeten.html>

<http://www.school-of-technology.de/Club-R2GS-SoSo-english.html>

