

INFORMATIK 2017 WS#13: 2nd GI/ACM Industry4.0 Security Standardisation Workshop on Industrial Automation and Control Systems (IACS)

Jan deMeer¹, Karl Waedt² und Axel Rennoch³

Abstract: Der 2^{te} internationale GI/ACM I4.0 Security Standardisation (ISS) Workshop auf der GI Jahrestagung 2017, fasst Sicherheits- gepaart mit Zuverlässigkeitsaspekten von Produktionsanlagen, z.B. in einer Smart Factory, die den Anforderungen der Multi-Teile-Norm IEC 62443[IEC14] für Industrielle Automatisierungs- und Kontrollsysteme (IACS) entspricht, genauer ins Auge. Industrieanlagen haben eine eigene inhärente Struktur, die in dem Referenz-Architekturmodell RAMI4.0 [ZVEI15], erstellt von einem Verbandsconsortium, geführt von ZVEI, skizziert ist. Diese Struktur fällt ins Gewicht, wenn ein Security-by-Design- Ansatz für verbundene, verteilte Industrieanlagen gewählt wird. Unter Sicherheit für IAC-Systemen werden hierbei im weitesten Sinne Systemeigenschaften und -fähigkeiten verstanden, die im sog. 'Pentagon of Trust' [JdM16] genannt werden, nämlich Vertrauen in vernetzte Produktionsanlagen und -geräten, Geheimhaltung von Fabrikationsdatensätzen, prüfbare Beachtung von Regulierungen und Gesetzen, Garantierung der Funktionalität von Produktionsanlagen und die einsichtige Anwendbarkeit von Anlagen und Geräten, was in ähnlicher Weise auch für vernetzte Geräte im sog. Internet der Dinge (IoT - Internet of Things) gilt. Der 2^{te} GI/ACM I4.0 WS strukturiert sich in die Handlungsgebiete: Architektur und Frameworks, Industrielle Erfahrung - Best Practice, Formalisierung und IACS Semantiken.

Keywords: Industrie4.0, IEC62443, Smart Factory, Cyber Security, Trustworthiness, Automation & Kontrolle, Real Time, Semantics, Graphen- Manipulations- Werkzeuge, RAMI4.0, FDT, IACS, IoT. Sicherheits- Indikatoren, ISO/IEC, ETSI Standards

1 Workshop Fundamente in der Normung

Der zweite GI/ACM Workshop für Sicherheits- Standards für Industrieanlagen (IAC-Systeme), wird besonders von den Arbeitsprogrammen der technischen Normungs-Komitees, international von der ISO/IEC, europäisch von der ETSI und national von den Normungsgremien der ISO/IEC JTC1 Mitgliedsländer, wie z.B. der DIN in Deutschland, geprägt.

Das Technische Komitee IEC TC65 'Industrial Process Measurement, Control and Automation' (IACS), beschreibt in seiner Anleitung zur 'Good Working Practice' [IEC07], wie man verantwortungsvoll Standards erzeugen kann und welche Rollen

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

² AREVA GmbH, Henri-Dunant-Str.60, 91058 Erlangen, karl.waedt@areva.com

³ FhG-FOKUS, Kaiserin-Augusta-Allee 31, 10589 Berlin, axel.rennoch@fokus.fraunhofer.de

vonnöten sind. Die Struktur des IEC TC65 spiegelt in ihren heutigen 4 Subkomitees und 8 Arbeitsgruppen, 3 vereinigten Arbeitsgruppen, 1 Advisory Gruppe und 2 ad-hoc Gruppen, die definitorische Problematik, IACS Standards zu schreiben, wieder. Es seien hier besonders die übergeordneten Themen der TC65 Unterkomitees: Industrielle Systeme (SC65A), Geräte der Mess- und Regelungstechnik (SC65B), Industrielle Netzwerke (SC65C) und Integration von Geräten in Unternehmens- (Management-) Systemen (SC65E), genannt. Aber auch in den vereinigten Arbeitsgruppen werden Anforderungs-Standards für Safety von IAC-Systemen, Energie-Effizienz in der industriellen Automatisierung (EEIA) und ein Referenzmodell für Smart Manufacturing, als auch ein Rahmenwerk für Systemarchitekturen für Smart Manufacturing, bearbeitet.

Das Normungskomitee ISO/IEC JTC1 SC27[ISO90] deckt den gesamten Bereich des Schutzes der Informations- (Privacy) und Kommunikations- (Security) Technologien (ICT) im allgemeinen, aber auch im besonderen für verbundene IAC-Systeme, ab. Der Normungsbereich des Subkomitees SC27 umfasst Methoden zum Erfassen von Sicherheitsanforderungen, ein Sicherheits- und Informations- Management für die ICT, kryptographische Mechanismen, um Eigenschaften der Informations- und Kommunikationstechnologien (ICT), wie Verantwortlichkeit, bzw. Nachvollziehbarkeit (accountability), Verfügbarkeit (availability), Integrität (integrity) und Geheimhaltung (confidentiality) verfügbar zu haben; ein Sicherheits- Management mit Registraturen für sicherheitsrelevante Systemkomponenten; ein Identity Management, Biometrische Verfahren und Informationsverarbeitung mit Privacy- Eigenschaften; Anforderungen an Konformanz- Verfahren zum Prüfen und Auditieren; Kriterien zur Evaluierung der Sicherheit in IAC Systemen.

2 Workshop Struktur

Der Workshop I4.0 Industrielle Sicherheitsnormung gliedert sich in folgende 3 Anwendungsbereiche:

1. **I4.0 Framework**, spricht die Folgen der Digitalisierung an, hervorgerufen durch die sog. 4. Industrielle Revolution, in den Beiträgen:
 - a. Integriertes Sicherheits- Framework - Ein holistischer Ansatz für IACS Sicherheits- Features;
 - b. IAC-Systemkomplexität im interdisziplinären Diskurs;
2. **I4.0 Practice**, wie sie von globalen industriellen stakeholder oder von national operierenden SMEs erfahren und ausgeübt wird, wird behandelt in den Beiträgen:
 - a. Herausforderung Interoperabilität und Sicherheit, ein Gegensatz?
 - b. Anwendung forensischer Methoden, wie RHEL, in Kritischen

Infrastrukturen;

3. I4.0 Semantik wird zur Verminderung von Mehrdeutigkeiten, wie sie in regulierten (EU Regularien, IT Gesetze, DIN Normen etc.) aber auch in geregelten (IACS) Systemen immer wieder zum Vorschein kommen, gebraucht. I4.0 semantische Fragestellungen werden in den Beiträgen:
 - a. über Sicherheit, Vollständigkeit, Indikatoren, Metriken - Ansatz einer einheitlichen SIEM Spezifikationsprache;
 - b. Formalisierung der Darstellung von Sicherheitseigenschaften.

behandelt.

Die vorgestellten drei I4.0-Anwendungsbereiche werden in 2 Sitzungen vorgestellt und diskutiert.

Literaturverzeichnis

- [ISO90] Normungskomitee ISO/IEC JTC 1 /SC 27 IT Security Techniques
https://en.wikipedia.org/wiki/ISO/IEC_JTC_1/SC_27#Scope, Gründung 1990.
- [IEC07] Normungskomitee IEC TC65 Industrial-process measurement, control and automation,
http://www.iec.ch/dyn/www/f?p=103:29:12055640240368:::FSP_ORG_ID,FSP_LAN_G_ID:1250,25#3, 2007.
- [IEC14] Normungsdokument IEC 62443-4-2 ed1: Industrial Communication Networks - Security for Industrial Automation and Control Systems - part 4-2 Technical Security Requirements for IACS Components, 2014 .
- [ZVEI15] Empfehlung ZVEI, VDI/VDE-GMA, DKE: Referenz-Architektur-Modell Industrie4.0 RAMI4.0: <https://www.zvei.org/themen/industrie-40/das-referenzarchitekturmodell-rami-40-und-die-industrie-40-komponente/>, 2015.
- [JdM16] Jan de Meer, smartspacelab.eu GmbH Berlin: 'The Pentagon of Trust' - Präsentation The BeST Model of Trustworthiness for Cyber Citizens, 2016