New Security Standards for Industrial Automation and Control Systems, based on IEC 62443-4-2 (IACS/SCADA) - Extended Abstract

Jan de Meer[1], Karl Waedt[2]

Abstract: Der von Industrie und Infrastrukturbetreibern erwartete vielteilige Standard IEC 62443, bzw. ISA99 [IEC TC57/WG15, IEC SC45A/WG9, ISO/IEC JTC1/SC27/WG1] für Industrielles Prozess-Management und Prozesskontrolle (IACS) besteht aus *4* Gruppen, mit bis zu *4* Teilen je Gruppe. Nur der vorläufig letzte Teil *IEC 62443-4-2*, der von den Normungsorganisationen Anfang 2016 zur Kommentierung ausgeschrieben worden ist, spielt im Rahmen der Diskussion um das Schlagwort *'Sicherheit für Industrie4.0'* [Aca13, BSI12c, PA15, BWE16] eine wichtige Rolle für Industrieanlagen und ist daher Hauptgegenstand der Betrachtung dieses Aufsatzes. Die anderen Teile der Industrienorm IEC 62443, bzw. ISA99, befinden sich in unterschiedlichen Entwicklungsstadien. Während die älteren, bereits publizierten Teile *g-p*:= 1-1, 2-1, 2-3, 2-4, 3-1, 3-3, bzgl. ihrer Aktualität in den Gremien, begutachtet werden, sind andere Teile in Planung begriffen, wie z.B. die Teile 1-4: *IACS security life cycle use cases*, 2-2: *IACS Security Management System*, alle anderen Teile sind in Arbeit.

Keywords: Sicherheits-Standard, IACS, SCADA, RAMI, Industrie4.0, Security Operation Center, Cyber-Angriffe

1 Einführung in Industrie-System-Referenzmodelle

Die Digitalisierung hat uns die 4. industrielle Revolution *Industrie4.0[Aca13, BSI12c, MH15]* und damit eine neue Betrachtungsweise von der kontrollierten industriellen Produktion, beschert. Die Organisationen BITKOM, VDMA, ZVEI u.a. haben für das Konzept *Industrie4.0* eine 'Umsetzungsstrategie' im sog. Referenz-Architekturmodell Industrie4.0 'RAMI' [Aca13, PA15, MH15] beschrieben, bzw. formalisiert.

Das RAMI beschreibt die Elemente von industriellen Produktionsanlagen (IACS) in 3 Dimensionen:

1. Das IT-Schichtenmodell (*Layers*) mit den, von unten nach oben 6 geschichteten IT-relevanten Aspekten: *Assets, Integration, Communication, Information, Functional,* bis einschließlich *Business*;

[1] smartspacelab.eu GmbH Abt. AIT, Berner Str. 21B, 12205 Berlin, demeer@smartspacelab.de
[2] AREVA GmbH, PEAS-G, Henri-Dunat-Str.50, 91058 Erlangen, karl.waedt@areva.com

2. Das zweistufige *Life-Cycle und Value-Stream* Produkt-Modell, wie es in der Empfehlung IEC 62890 steht, bestehend aus den aufeinanderfolgenden Phasen: Produkttypenetwicklung, die in Produktionsprozesse von Produkttyp-Instanzen überführt werden;

3. Das 7-Hierarchien-Anlagen-Modell (*Plant Hierarchy Levels*), nach IEC 62264 oder IEC 61512, mit den technisch-organisatorischen Kontrollstrukturen von Produktionsanlagen: *Product, Field Device, Control Device, Station, Work Centers, Enterprise, Connected World*;

Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) spezifiziert in [BSI12c], welchen höchsten Kritikalitäten [JdM14], d.h. Top-10 der kritischen Bedrohungen, *Industrial Automation and Control Systems (IACS),* ausgesetzt sein können: unberechtigte Nutzung von Fernwartungszugängen; online-Angriffen über die RAMI-Anlagen-Hierarchien; Angriffe auf Commercial *off-the-shelf (COTS)* IT-Komponenten; *DDoS*-Angriffe zur Störung von hierarchischen *IACS*-Kontrollstrukturen; Fehlverhalten und Sabotage von innen und außen einer Industrie-Anlage; Schadkode-Angriffen, mittels mobiler *IT*-Komponenten; *Man-in-the-middle (MiM) Attack*; nicht-autorisierter Zugriff auf *IACS*-Ressourcen; Angriffe auf allen IT-Schichten; Technisches Fehlverhalten und höhere Gewalt im gesamten *RAMI*-Raum.

SCADA - Supervisory Control and Data Acquisition [BWE16, TC11[3]] - wird seit Jahren weltweit in fast allen Arten Industrieller Produktionsprozesse verwendet. Eine sog. SCADA-Anwendung mißt Indikatordaten einer Anlage, um das System zu steuern bzw. zu kontrollieren. Sie besteht also aus den Teilen, (a) den überwachten Komponenten (sog. *Controls*), z.B. Verkehrsampel oder einer Energieversorgungsanlage, etc. (b) den Komponenten zur Überwachung (sog. *Intelligent Devices*), z.B. Sensoren und Aktoren (sog. *Remote Telemetry Units*) und einer Leitwarte (sog. *Security Operation Center, SCADA Master Units, ...*) und (c) einem Kommunikationsnetzwerk, das *SMUs (SOCs)* und *RTUs* im Feld miteinander verbindet.

2 Der IACS Sicherheitsstandard IEC 62443-4-2

Der vorläufig letzte Teil *IEC 62443-4-2* [IEC15a][1] des vielteiligen 'Industrie-Standards',

[3] In [16] stellt Siemens sein eigenes *SIMATIC SCADA System* für das Engineering großer Produktionsanlagen, vor. Es eignet sich als Entscheidungswerkzeug für Systemoptimierungen, es ist skalierbar zur Integration bestehender Anlagen, es kann mit der vorhandenen IT integriert werden, es bietet jederzeit Zugriff auf alle Anlagedaten. Für die Sicherheit, Zuverlässigkeit und Verfügbarkeit der Anlagedaten stehen geeignete Funktionen zur Verfügung. SIMATIC SCADA ist in vielen Branchen universell einsetzbar, u.a. Automobilindustrie, Stahlindustrie, Druck, Logistik, Transport, Verkehr, Öl-, Gasversorgung, Gebäudetechnik, Chemie, Pharmazeutik etc.

[1] Sowohl, im, von den Autoren benutzten Referenzdokument .../SC27/WG3 N1178, als auch im Dokument DKE 716.0.1, wird der Titel 'Security for Industrial Automation and Control Systems (IACS)' verwendet; Teil 4-2, worauf sich die Autoren in diesem Artikel beziehen, ist mit 'Technical Security Requirements for IACS Components' betitelt.

wird in erster Linie nicht mit Schnittstellen zwischen Mensch und Maschine (*Human-Machine-Interaction*) in Verbindung gebracht; jedoch spielt der *HMI*-Faktor dennoch eine gewichtige Rolle, nämlich dadurch, daß das Potenzial eines möglichen Angreifers auf ein reales Industrielles Automatisiertes, Kontrolliertes Produktionssystem (*IACS/SCADA)*, in 4 Stufen des Aufwandes, den sog. *Security Levels* im Konzept der Cyber-Abwehr, eingeteilt wird.

Die Evaluierung Industrieller Automatisierung und Überwachungssysteme (*IACS/SCADA*), gestützt auf *benchmarking*, zielt ab, auf den Nachweis der operativen Nachhaltigkeit, bzw. des Erhalts der Funktionsfähigkeit in einer rauen Umgebung, die sich auf 4 verschiedenen Intensitätsstufen, die hier nicht weiter betrachtet werden können, stützt.

Der betrachtete, spezifische Standard IEC 62443-4-2 für die Sicherheit von *IACS* Komponenten, muss die Definition von Sicherheits-Anforderungen auf den gesamten *RAMI*-Raum (s. Kapitel 1) von Entwicklung und Produktion, plus die gesamte *RAMI*-Produktionshierarchie, vernetzt durch die IT-Schichten, erfüllen.

3 Sicherheits-Indikatorklassen für Produktionsanlagen

Der Standard-Entwurfsteil *IEC 62443-4-2* [IEC15a] spezifiziert die erforderlichen Sicherheits-Anforderungen für identifizierte *IAC* -System -Komponenten, *component requirements (CR)*, die zusätzliche Vorschläge enthalten können, wie man Sicherheitsanforderungen verbessern kann, sog. *requirement enhancements (RE)*. Die Sicherheitsanforderungen für Komponenten werden in 4 Sicherheits-Levels (SL) kategorisiert, welche die Anforderungen von 7 sog. grundsätzlichen Anforderungen, *foundational requirements (FR)*, erfüllen. Die *FR* stehen im Einklang mit 51 System-Anforderungsgruppen, *system requirements (SR)*.

IEC 62443-4-2 enthält Vorschläge für 7 Maßnahmefelder, *foundational requirements (FR)* genannt, die bei branchen-übergreifenden Sicherheits-, bzw. *hardening* Massnahmen oder Tests, in Betracht zu ziehen sind.

In einer angenommenen verletzlichen Umgebung ist jedes dieser *7 foundation requirements (FR)* Angriffen unterschiedlicher Intensität, wie in den *security levels (SL)* beschrieben, ausgesetzt. SL 1 bis 4 geben den Aufwand an, den man treiben muss, um, innerhalb einer spezifischen Sicherheitsmassnahme, *FR 1 bis 7*, alle Angriffe der Stärke *SL 1 bis SL 4* abzuwehren.

4 Ergebnisse und Ausblicke

Zusammenfassend, in Bezug auf das obige Beispiel $FR_{(j=6)}$, lässt sich sagen, dass für Tests des Maßnahmenbereichs FR_6=*TRE*, d.h. 'zeitgerechte Antworten auf

sicherheitsrelevante Ereignisse', z.B. auf der Sicherheitsstufe *SL2:*= 'geringe Motivation der Angreifer', *benchmarks*, bzw. *Audits* durchgeführt werden, die die Ausführung von *IACS* Operationen über einen bestimmten Zeitraum überwachen (*monitoring*) und über alle beobachteten Verstösse (*incidents*) gegen die Sicherheitsanforderungen Meldung geben, als auch Beweise zur Durchführung von nachfolgenden forensischen Untersuchengen sicherstellen.

In einem implementierten *benchmark* können die tatsächlichen Sicherheitsverstöße (*incidents*), z.B. für die Sicherheitsstufe *SL2*, die darin bestehen, dass nicht-autorisierte Personen oder Prozesse versuchen, sich Zugang oder Zutritt zu geschützten Daten oder Räumen zu verschaffen versuchen.

In Ergänzung zur sog. *SIEM-Landschaft* und um Ausdrucksstärke für die Definition von Sicherheitsereignissen und das Ereignis-*SIEM*-Management herzustellen, gibt es Bedarf für eine eigene *'SIEM-Sprache'*, in dem besprochenen Kontext ***'C**ommon **S**IEM **lang**uage'*, kurz *'C-Slang'* (nicht Teil dieser Betrachtungen, ist aber geplanter *New Work Item (NWI)*, der *ETSI Industrial Specification Group for Information Security Indicators ISG ISI* bis Ende 2017).

In der Tat, spricht u.a. der Technische Report *WD 19608:2015-07-15* [ISO15] von einer ***C**ommon language*, die es für die Kommunikation zwischen den Systemteilhabern Konsument, Entwickler und Evaluatoren, sowohl für *security,* als auch für *privacy*, zu realisieren gilt.

Die vollständige Spezifikation der 7 *IACS*-Operationsfelder mit jeweils k_j Komponenten (s. 7 lists of *CR-benchmarks*), welche die Basis der *SIEM*-Landschaft bildet, werden in nachfolgenden normungsnahmen Vorhaben behandelt und publiziert. Diese *benchmarks* sind jedoch für alle *KMUs* wichtig, weil sie die Grundlage für den sicheren und zuverlässigen Betrieb von industriellen Produktionssystemen und -plattformen (*IACS*), bilden.

Literatur

[ISI13a] ETSI GS ISI 001-1/2 (2013)Information Security Indicators (ISI) – Indicators (INC) Part 1 „A full set of Operational Indicators for Organizations to use to benchmark their security posture“ & ISI INC Part 2 „Guide to select Operational Indicators based on the full set given in INC part 1“

[ISI13b] ETSI GS ISI 002 (2013) Information Security Indicators (ISI) – Security Event Model (SEM) „A Security Event Classification Model and Taxonomy“

[IEC15a] IEC 62443-4-2 Ed.1 Security for Industrial Automation and Control Systems (IACS) part 4-2: Technical Requirements for IACS components (IEC/TC57/WG15, SCA45A/WGA9, ISO/IEC JTC1/SC27/WG3 N1178 (2015-07) IT ST - Security Evaluation, Testing and Specification), https://webstore.iec.ch/preview/info_iec62443-2-4%7Bed1.0%7Db.pdf

[ISO15] ISO/IEC WD19608:2015-07-08] ISO/IEC JTC1 SC27 WG3 N1193: IT ST Guidance for Developing Security and Privacy Functional Requirements based on ISO/IEC 15408

[JdM15] Jan deMeer, ssl.eu GmbH Berlin: "Mehr Datenschutz und Betriebssicherheit durch Cyber Security Testing", ASQF SQ Magazin Ausgabe 34, März 2015, S.28-31

[WDG15] K. Waedt, Y. Ding, Y. Gao, X. Xie: I&C Modeling for Cybersecurity Analyses, 1st TÜV Rheinland China Symposium - Functional Safety in Nuclear and Industrial Applications, Shanghai, 2015-10

[BSI12a] Bundesamt für Sicherheit in der Informationstechnik (BSI): ICS Security top-10 Self-check - Machen Sie den Test, wie sicher ist Ihre Industrial IT?

[BSI12b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Empfehlung: IT in der Produktion - Industrial Control System Security, top-10 Bedrohungen und Gegenmassnahmen, BSI-CS100|v1.00, 29.5.2012

[IEC15b] IEC 2015 NP 62443-3-2 - 65/611/NP - Security for Industrial Automation and Control Systems - Par 3-2: Security Risk Assessment and System Design

[Aca13] Acatech, Forschungsunion: Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 - Abschlußbericht des AK Industrie4.0, BMBF April 2013

[BSI12c] BSI Empfehlung: IT in der Produktion - Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen; BSI-CS10 | Version 1.00, 29.5.2012

[PA15] Peter Adolphs: RAMI4.0 - An Architectural Model for Industrie4.0, DIN Berlin, 18.6.2015

[MH15] Michael Hoffmeister, Festo AG&Co.KG: ZVEI The Industrie4.0 Component, Version 1.0 April 2015

[JdM14] Jan deMeer, smartspacelab.eu GmbH Berlin: Dynamische Kritikalitätsbewertung von Prozessen in Kritischen Infrastrukturen, GI/ACM RG BB White Paper 3.2.2014, linkedin;

[BWE16] BM f. Wirtschaft und Energie: IT-Sicherheit für die Industrie4.0; Abschlußbericht zur Studie im Auftrag des BMWE, Januar 2016;

[TC11] DPS Telecom, Fresno CA 93727-1523 USA: SCADA Tutorial Version 2.0, released August 8, 2011 - White Paper, www.dpstelecom.com;

[Sim14] Siemens.de/scada: SIMATIC SCADA Systeme, Artikel Nr. E20001-A830-P810, Siemens AG 2014