Security and Privacy Benchmarking based on IEC 62443-4-2

Jan B. de Meer[1] · Karl Waedt[2]

[1]smartspacelab GmbH
demeer@smartspacelab.de

[2]AREVA GmbH
Karl.Waedt@areva.com

Zusammenfassung

Der 2. Teil der 4 Gruppen umfassenden, mehrteiligen Norm *IEC 62443-4-2* (Teil 4-2 des Standards IEC 62443, bzw. ISA99, liegt in der Edition *1.0 2015-06* im Entwurf *ISO/IEC JTC1/SC27/WG3 N1178 (2015-07)* den Autoren [IEC15] vor; bzw. können alle fertigen Normenteile kostenpflichtig von nationalen oder internationalen Normungsorganisationen besorgt werden) – wird gerade in den internationalen Gremien diskutiert und frühestens Ende 2016 veröffentlicht werden. Die betrachtete *IEC*-Norm hat, nach Mg. der Autoren, Bezug zur Industrienormenserie *ETSI GS ISI-001-1/2 -002* [MeRR15], *-003* [WDGX15] mit der Katalogisierung von *Information Security Indicators (ISI).* Damit wird eine Brücke zwischen *Component Requirements (CR)* der *IEC 62443-4-2*-Norm und den *Information Security Indicators* (*ISI)* der *ETSI-GS*-Empfehlungen geschlagen. Es lässt sich bereits heute absehen, dass diese Norm für *Industrie4.0*-Plattformen [BMBF13, BSIC12], sowie für Implementierungen von Sicherheitsanforderungen für ein industrielles automatisiertes und kontrolliertes Produktionssysteme (*IACS*), eine entscheidende Rolle spielen wird. Daher beschäftigt sich das betrachtete Normungsprojekt mit der Methode des *Sicherheits&Privacy Benchmarking* auf der Grundlage der Empfehlung *IEC 62443-4-2* [IEC15] und *ETSI GS ISI* [ETSI01, ETSI02], die Entscheidern, *SOC/SIRT*-Managern in *KMUs* sowie in großen Organisationen, z.B. *Smart Cities*, Bewertungs- und Testmittel an die Hand gibt. Damit können für den sicheren und zuverlässigen Betrieb von industriellen, *smarten* Systemen und Infrastrukturen, nachhaltige Entscheidungen vorbereitet und verantwortlich ausgeführt werden.

1 Einleitung

Die Digitalisierung hat uns die 4. industrielle Revolution *Industrie4.0* und damit eine neue Betrachtungsweise von der Produktion und von Kontrollanlagen beschert. Die Organisationen BITKOM, VDMA und ZVEI haben für Industrie4.0 eine 'Umsetzungsstrategie' im sog. Referenz-Architekturmodell Industrie4.0 'RAMI' [BMBF13, Adol15, Hoff15] beschrieben, bzw. formalisiert.

Das RAMI beschreibt die Elemente der industriellen Produktion in 3 Dimensionen:

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

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 253-263.

2. Das zweistufige *Life-Cycle und Value-Stream* Produkt-Modell, wie es in der Empfehlung IEC 62890 steht, bestehend aus den Phasen: Produkttypentwicklung, 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 [BSIC12], welchen höchsten Kritikalitäten [Meer14], d.h. Top-10 der kritischen Bedrohungen, *Industrial Automation and Control Systems (IACS),* ausgesetzt sein können:

1. unberechtigte Nutzung von Fernwartungszugängen, was z.B. die unteren RAMI-Schichten *Assets, Integration* besonders gefährdet;
2. online-Angriffe über die RAMI Anlagen-Hierarchien: *Enterprise, Connected World*;
3. Angriffe auf Commercial off-the-shelf (COTS) IT-Komponenten, wie Betriebssysteme, Application Server, DB etc., auf den RAMI-Schichten *Integration, Communication, Information*;
4. *DDoS*-Angriffe zur Störung von hierarchischen Kontrollstrukturen in Industriellen automatisierten und kontrollierten Produktionssystemen (IACS), wie *Field Device, Control Device, Station, Work Centers* etc.
5. Fehlverhalten und Sabotage von innen und außen einer Industrie-Anlage, bzgl. der Schutzziele Vertraulichkeit und Verfügbarkeit, in der Spanne (RAMI-Raum) zwischen *Life Cycle* Entwicklung und Produktion, den IT-Schichten *Functional, Business* und den spezifischen Produktionshierarchien *Work Station, Centers, Enterprise, Connected World*;
6. Schadkode-Angriffen, mittels mobiler IT-Komponenten, werden auf den Produkt- bzw. Anlagenhierarchien *Product, Field Device, Control Device, Station* ausgeführt;
7. *Man-in-the-middle (MiM) Attack*, durch nicht-autorisiertes Lesen oder Verändern von Automatisierungs- und Kontrollanweisungen innerhalb einer IACS-Anlage;
8. nicht-autorisierter Zugriff auf *IACS* Ressourcen auf allen 7 Produktionshierarchien, von Innentätern, durch Manipulationen, z.B. von Authentizitätsprüfungsverfahren und -daten auf den IT-Schichten Information, Functional, Business;
9. Angriffe auf allen IT-Schichten, um Netzwerkkomponenten zu manipulieren;
10. Technisches Fehlverhalten und höhere Gewalt im gesamten RAMI-Raum.

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

Der Sicherheits-Standard, bzw. -Norm für IACS Komponenten ist eingebettet in den vielteilige Standard IEC62443, bzw. ISA99 [Referenzdokument: IEC TC57/WG15, IEC SC45A/WG9, ISO/IEC JTC1/SC27/WG1] für Industrielles Prozess-Management und Prozesskontrolle besteht aus $g=4$ Gruppen, mit bis zu $p \leq 4$ Teilen je Gruppe und ist im Rahmen der Diskussion um das Schlagwort *'Industrie4.0'* [BMBF13] Gegenstand der Betrachtung dieses Aufsatzes.

Gruppe Nr.1 *'General'* von *IEC62443-g-p,* enthält die Normenteile für die verwendete Terminologie, Glossare, Metriken zur Komplianz-Bewertung der Systemsicherheit und formal beschriebene Anwendungsfälle (*use cases*); Gruppe Nr.2 *'Policy and Procedures'* enthält die Teile für die Anforderungen an ein Sicherheits-Management, Anleitung zur Implementierung, Patch-Management u.a.; Gruppe Nr.3 *'System'* enthält die Teile, die Sicherheitstechnologien, Sicherheits-Levels für Zonen und kontrollierten Kommunikationsbeziehungen zwischen Zonen (*conduits*) definieren; Gruppe Nr. 4 *'Component'* enthält die Teile zur Produktentwicklung unter Berücksichtigung technischer Sicherheitsanforderungen.

Der vorläufig letzte Teil *IEC 62443-4-2* [IEC15][1] des vielteiligen Standards, wird in erster Linie nicht mit Schnittstellen zwischen Mensch und Maschine (*Human-Machine-Interaction*) in Verbindung gebracht; der menschliche Faktor spielt dennoch eine gewichtige Rolle, weil das Potenzial eines möglichen Angreifers auf ein reelles Industrielles Automatisiertes Kontrolliertes Produktionssystem (IACS*)*, in den 4 Stufen der sog. *Security Levels* (s. Abbildung 1: *SL*-Dimension der Angriffsmotivation) im Konzept der Cyber-Abwehr, seinen Niederschlag findet.

Die anderen nicht-*HMI*-spezifischen Dimensionen der Cyber-Abwehr auf IACS bestehen aus a) 7 Klassen *Foundational Requirements* (FR_j $|j=1,...7$), und b) für jede Klasse, eine Gruppe sog. *Component Requirements (CR)*, insgesamt 53 *CR*. Für alle *CR* pro *FR* (s. nächster Abschnitt) müssen Sicherheits-Tests und *benchmarks* für folgende technischen Sub-Infrastrukturen inform von Testnormen entwickelt und angewendet werden:

1. Applikationen (*ACR*);
2. Eingebettete Systeme (*ECR*);
3. Host Anlagen und Geräte (*HCR*);
4. Netzwerk Infrastrukturen (*NCR*).

Die Evaluierung Industrieller Automatisierung und Überwachungssysteme (*IACS*), gestützt auf Benchmarking, zielt auf den Nachweis der operativen Nachhaltigkeit, bzw. des Erhalts der Funktionsfähigkeit in einer aggressiven Umgebung, die auf verschiedenen Intensitätsstufen operiert, ab:

1. ununterbrochene Unterstützung essentieller Funktionen, bei Ergreifung von Gegenmaßnahmen in Sicherheitsvorfällen;
2. Komponenten, die sich auf kompensierende Gegenmaßnahmen stützen, sollen den besonderen Anforderungen an Sicherheitszonen (*zones*[2]) und geschützten Kommunikationskanälen zwischen Zonen (*conduits*[3]) in *IEC 62443-3-2* [IECN15] genügen, (Anmerkung: Der Normenteil 3-2 [IECN15] ist nicht Gegenstand der auf Teil 4-2 [IEC15] beschränkten Betrachtungen).
3. alle *IACS* Komponenten sollen die Fähigkeit haben, das Konzept der geringsten Befugnisse (*concept of least privilege*) durchzusetzen;

---

[1] Sowohl, im von den Autoren benutzten Referenzdokument .../SC27/WG3 N1178, als auch in 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.

[2] Eine *zone* ist eine Gruppe von Entitäten, die einer Aufteilung des Gesamtsystems nach funktionalen, logischen oder physikalischen, auch örtlichen Gesichtspunkten, entsprechen;

[3] Ein *conduit* ist eine lokale Gruppierung von Kommunikationskanälen, die gemeinsamen Sicherheitsanforderungen genügen, zwischen 2 oder mehreren Zonen.

4. überwölbende *CR*-Anforderungen:
   - Unternehmenswerte, die mittels funktionaler Sicherheit geschützt werden müssen, sollen Plattform- und Hardwaresicherheiten aufweisen;
   - Vertrauen erzeugende Maßnahmen (*trust provisioning*) umfassen:
   - schützenswerte Werte (*assets*) die geheim zu halten sind, z.B. *private keys, asymmetric signature scheme* etc.
   - schützenswerte Werte, die unantastbar und authentisch bleiben müssen, z.B. *public key* einer autorisierten Einrichtung, *configurations settings* etc.
   - *Privacy* soll für Geräte und Anwendungen nachhaltig bestehen bleiben; *privacy* ist mehr als Datenschutz (*data protection*), denn es beinhaltet auch Unverlinkbarkeit (*non-linkability*) und Nicht-Nachverfolgbarkeit (*non-traceability*); ein in Betrieb genommenes System soll in seiner Umgebung, Gesetze und Regulationen, die gerade in Kraft sind, nicht einschränken oder gar verletzen.

2 Sicherheits-Indikatoren relevante Standards

Im folgenden Abschnitt werden bzgl. der Vermessung von *'Industrie4.0-Plattformen',* [BMBF13] einige (nach Mg. der Autoren) relevante Publikationen und Empfehlungen der *ETSI*, *ISO/IEC* und anderer Organisationen, z.B. Bundesministerium Wirtschaft & Energie[BMWE16], kurz vorgestellt:

1. Standard [ETSI01], eine Empfehlung der ETSI ISG ISI, enthält Indikatoren für kritische Sicherheitsvorfälle, die folgenden Ereigniskategorien zugeordnet werden können:
   - Eindringversuche, Angriffe von außen (*Intrusion – ISI Category IEX*) Fehlfunktionalität (*Malfunctioning – ISI Category IMF*)
   - Von der Norm abweichendes internes Verhalten (*Deviant Behavior – ISI Category IDB*)
   - Verhaltensbedingte Gefährdung (*Vulnerability – ISI Category VBH*)
   - SW-bedingte Gefährdung (*Vulnerability – ISI Category WSW*)
   - Konfigurations-bedingte Gefährdung (*Vulerability – ISI Category VCF*)
   - Verletzung allgemeiner Sicherheitsregeln bedingte Gefährdung (*Vulnerability – ISI Category VTC/VOR*).
2. Ebenfalls eine Empfehlung der ETSI ISG ISI ist das Dokument [ETSI02], welches in Bezug zur Norm ISO/IEC 27004 steht. Die Empfehlung beschreibt ein *„Information Security Measurement (ISM)“* -Modell, das die unterschiedlichen Bewertungs- und Darstellungsweisen (Attribute) von komplexen, *high-level Security Governance*-Vorgängen und einfachen technischen Messgrößen, mittels einer Übergangsdarstellung, miteinander verbindet. Die Attribute der Übergangsdarstellung der Indikatoren sind: Auswahl eines geeigneten Abstraktionsgrads – gleichwertige Anwendbarkeit für Ereignisse, die System-Gefährdung (*Vulnerability*) und kritische Zwischenfälle (*Incident*) betreffend – Ausführung einer umfassenden und konsequenten Taxierung und Einhaltung der Verständlichkeit für alle beteiligten Teilhaber – Reduzierung der Komplexität, indem komplexe Sicherheits-relevante Zwischenfälle in einfachere Vorgänge zerlegt werden können [ETSI02].
3. Der von der *IEC* vorgeschlagene Teil 4.2 des internationalen Multi-Standards *IEC 62443-*

4-2 [IEC15] für Sicherheit Industrieller Automations- und Kontrollsysteme (*IACS*), stellt dar, wie eine Produktionsanlage mit nicht-*IACS*-spezifischen Netzwerken sicher und zuverlässig interagieren kann. Die Komplexität dieser Verbünde bietet jedoch Angreifern immer mehr Gelegenheit, in *HW*- und *SW*-Komponenten einzudringen. Diese Schwächen könnten in aktivierten technischen Plattformen, wie in den Bereichen Gesundheit, zuverlässigen Systemen oder Umwelt (*HSE*)[4], leicht zu Vertrauensverlusten führen. Daher zielen *IACS*-Sicherheitsanforderungen besonders auf Verfügbarkeit der Systeme und Schutz der Betriebsgelände, gerade auch auf niedrigem Sicherheits-Level aber ebenso in Systemen mit zeitkritischem Antwortverhalten.

4. Im Interview des *SQ*-Magazins, enthalten in [MeRR15], stellen die Autoren dieses Artikels das 'Informations- Sicherheits- Indikatoren' (*ISI*) Schema der *ETSI ISG ISI* vor. Die Einteilung der Indikatoren richtet sich nach Indikatorklassen der *Common Criteria* und enthält selbst die 3 großen Klassen: *'Incidents', 'Vulnerabilities' und 'Impacts'*. Diese Klassen enthalten eine Vielzahl operativer Maßnahmeklassen, die mit messbaren Attributen versehen sind.
5. Der Beitrag [WDGX15] des *AREVA*-Forums, stellt industrielle *ISMS*-geeignete Werkzeuge und Plattformen, z.B. das sog. 'TXS-based Protection System', das für den Reaktorschutz geeignet ist, vor. Damit werden in sog. technischen Feldern bzw. Inseln, wie Nukleareinrichtungen, Turbinen oder Gebäudetechnik, jeweils gespeist von elektrischen Energiesystemen, *Cyber Security* Maßnahmen in vergleichbarer Art und Weise ausgeführt. Das hat den Vorteil, dass die Reports mit den Nachweisen des Erfolgs oder Misserfolgs der Maßnahmen, unabhängig vom Vorhandensein technischer Inseln, dargestellt werden können.
6. Bereits 2012 hat das *BSI*, jedoch bezugnehmend auf die *ISO270nn*-Serie, *VDI/VDE2181* und den eigenen 'IT-Grundschutz-Maßnahmen-Katalog [*www.bsi.de/gshb/*], weitere Maßnahme-Empfehlungen zu den top-10-Bedrohungen der 'IT in der Produktion' herausgegeben, s. [BSI12, IECN15]. Das Unternehmen, das eine Bestandsaufnahme der Sicherheit der implementierten Industrie-*IT* vornimmt, bewertet für jede einzelne Maßnahme der top-10-Bedrohungen ihre Umsetzung in der Produktion.
7. Der Standard *IEC 62443*, kommt den vorgenannten top-10-Bedrohungs-Szenarios, nur dann zum Zuge, wenn das Bewertungsergebnis zeigt, dass alle Maßnahmen bereits w.o.w. 'vollständig umgesetzt' worden sind. Der *IEC 62443* wird hier als 'ganzheitlicher Ansatz' betrachtet, mit dem man ggf. systematisch, weiter ins Detail gehen könnte. Das BSI betrachtet als Voraussetzung zur Durchführung des beschriebenen Selbst-Prüfverfahrens der eignen *ICS*-Sicherheit, die Bestätigung sog. 'Basisfragen' durch das Unternehmens-Management, nach dem Vorhandensein von Ansprechpartnern der *IT*-Sicherheit, eines Risikomanagements, *ICS*-Anlagen-Netzplans, von Anlagen-Schnittstellen, Meldeverfahren, Verbesserungsprozessen für Schwachstellen und eines Notfallsmanagements.
8. Im Januar 2016 hat das Bundesministerium für Wirtschaft und Energie den Abschlussbericht einer Studie zur 'IT-Sicherheit für die Industrie4.0'[BMWE16] publiziert. Darin

[4] Plattformen für HSE und IACS dienen zwar unterschiedlichen Anwendungen, die vorgestellte Norm geht aber davon aus, dass unterschiedliche Plattformen auch miteinander in Interaktion treten können.

verweist es auf Risiken, die Betreiber einer I4.0-Plattform, bzw. Infrastruktur, zu berücksichtigen haben:

a. dynamische, organisations- und länderübergreifende Vernetzung von Industrieanlagen;
b. Mitteilung, bzw. Erhebung von Teilnehmer- und Gerätedaten aus funktionalen Gründen, die u.U. als Geschäftsgeheimnis gelten oder worauf Datenschutz- und IT-Sicherheits-Regularien angewendet werden müssen;
c. I4.0-Infrastrukturen, die aufgrund von Ereignissen aus verschiedenen Domänen und Subsystemen, sicherheitsrelevante Entscheidungen autonom treffen können;

Daraus ergeben sich 36 Handlungsvorschläge, bzw. Szenarien, die von folgenden I4.0-Teilhaber (stakeholder) -Gruppen berücksichtigt werden müssen:

a. Unternehmen und Branchenverbände
b. Politik und Gesetzgeber
c. Aufsichts- und Regulierungsbehörden
d. Standardisierungs- und Normierungsorganisationen.

3 Indikatorklassen für Produktionsanlagen

Der Standard *IEC 62443-4-2* [IEC15] enthält Vorschläge für folgende 7 Felder, *foundational requirements (FR)* genannt, die bei branchen-übergreifenden Sicherheits-, bzw. *hardening* Maßnahmen und Tests, in Betracht zu ziehen sind:

1. IAC (identification and authentication control): Identifikations- und Authentizitäts-Kontrolle;
2. UC (use control): Benutzungskontrolle von Ressourcen;
3. SI (system integrity): System-Unverletzlichkeit (Integrität);
4. DC (data confidentiality): Datenschutz und Geheimhaltung;
5. RDF (restricted data flow): Eingeschränkter kontrollierter Datenfluss
6. TRE (timely response to events): Reaktion auf Ereignisse in angemessener Zeit
7. RA (resource availability): hinreichende Verfügbarkeit von IKT-Ressourcen.

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 4* abzuwehren:

1. *SL1* enthält Angriffe über Lecks in Kommunikationskanälen (*eavesdropping*) oder unbeabsichtigtes Preisgeben von Informationen (*casual exposure*), die Angreifer ausnutzen können;
2. *SL2* beschreibt Angriffe einer Einheit, die aktiv nach Informationen sucht und dabei einfache Hilfsmittel mit geringem Aufwand, d.h. Ressourcen gebraucht, auf der Grundlage grundsätzlicher Kenntnisse mit geringer Motivation;
3. *SL3* beschreibt Angriffe einer Einheit, die aktiv nach Informationen sucht und dabei komplexe Hilfsmittel mit moderatem Aufwand, d.h. Ressourcen gebraucht, *IACS*-spezifische Kenntnisse besitzt und mit moderater Motivation vorgeht;

4. *SL4* beschreibt Angriffe einer Einheit, die aktiv nach Informationen sucht und dabei komplexe Hilfsmittel mit hohem Aufwand, d.h. Ressourcen gebraucht, *IACS*-spezifische Kenntnisse besitzt und mit hoher Motivation vorgeht.

Natürlich sind nicht alle *FRs* gleich gut geeignet *SL3* oder *SL4*-Angriffe abwehren zu können. Erst im Verbund, d.h. wenn alle 7 *FRs* implementiert sind, ergibt sich eine gute Chance, auch SL4-Angriffe erfolgreich abwehren zu können.

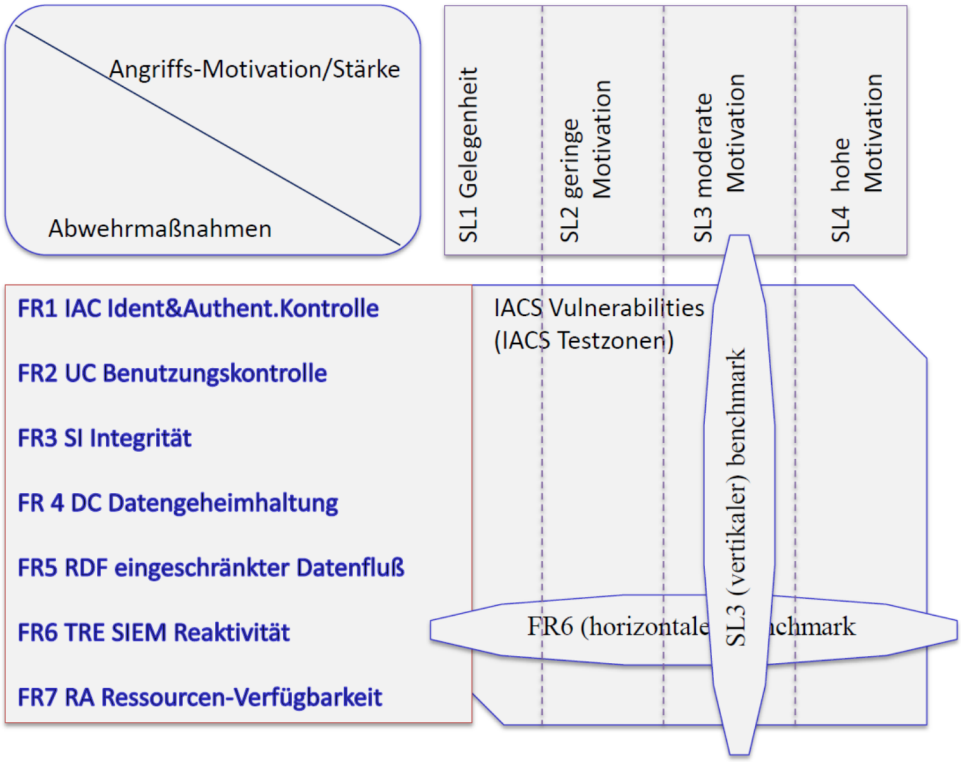

Abb. 1: *IACS* Benchmarking und Testzonen

In Abbildung 1 ist die "*IACS*-Testzone" dargestellt. Sie besteht aus den IACS-Indikatorklassen *FR1* bis *FR7*, die bzgl. der Sicherheitsstufen *SL1* bis *SL4* zu prüfen sind. So soll z.B. für die Indikatorklasse FR6 'SIEM Reaktivität auf der Stufe *SL3'* ein *benchmark* entworfen werden. *SL3* bedeutet die moderate Annahme, dass z.B. Kenntnisse über den Zugang zur Produktionsstätte aber keine Kenntnisse über Steuerungsmechanismen der Produktion, an Dritte, nicht autorisierten Personen, gelangt sind.

Entsprechend ist das $FR_{(j=6)}$ *TRE benchmark* zu entwerfen (beachte: *benchmark* entspricht im IACS-wording einem *'component requirement'* und wird mit $CR_{j.i}$ bezeichnet):

- *CR6.1*: Prüfung der vorgezeigten Autorisierung von Personen, Prozessen oder verwendeten Test-Werkzeugen, die es ihnen gestattet, jederzeit lesend auf *IACS*-Datenbestände, z.B. Sicherheits-Audit-logs, zugreifen zu können; *CR6.1*-Indikatoren sind Autorisierungsdaten, gebunden an Subjekte und Objekte. Sie können korrekt, fehlerhaft, gestohlen oder gefälscht sein. Für *SL3* bedeutet das, dass gefälschte, gestohlene oder fehlerhafte Autorisierungen erkannt und zurückgewiesen werden müssen.
- *CR6.2*: Sofern ein Gerät oder eine Anwendung sicherheitsrelevante Bedeutung für die gesamte Produktionsanlage besitzt (d.h. ein *asset* darstellt), müssen diese *IACS*-

Komponenten kontinuierlich überwachbar sein. Die Prüfung dieser Anforderung geschieht, indem eingesetzte Techniken oder industrielle Praktiken dahingehend überprüft werden, ob mit ihnen das Auffinden und die Berichterstattung über Sicherheitsverletzungen zeitlich angemessen durchgeführt werden kann.

Der *CR6.2*-Indikator ist zum einen, ein kontinuierlicher Datenstrom einer sicherheitsrelevanten *IACS*-Komponente (*asset*), der auf Abweichungen vom unkritischen Verhaltensmuster permanent korreliert wird; und zum andern, die gemessene Zeit, die vergeht, vom Zeitpunkt des Erkennens einer kritischen Verhaltensabweichung $t_{critical}$ dem Zeitpunkt der Erstellung einer Analyse $t_{Analyse}$, bis zum Zeitpunkt der Reaktion des zuständigen *SOC/SIRT* $\boldsymbol{t_{SIRT}}$:

$$(t_{SIRT} - t_{Analyse}) + (t_{Analyse} - t_{critical}) = T_{SIRT} + T_{Analyse};$$

wobei $T_{Analyse}$ die Zeit in der die *correlation*[5] und T_{SIRT} die Zeit, in der die Reaktion evaluiert werden, jeweils ist.

Für *SL3* zum Beispiel, bedeutet das, dass ein Angriffsversuch auf ein *IACS-asset*, in hinreichender Detektionszeit $T_{SIRT} + T_{Analyse}$ entdeckt und verhindert werden soll.

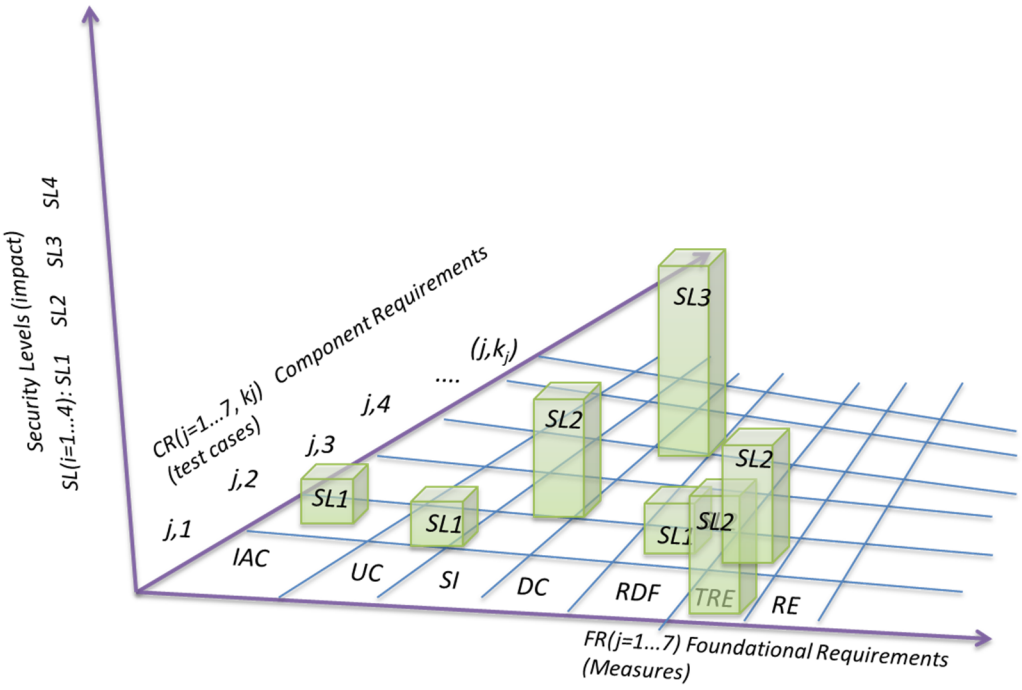

Abb. 2: CR Benchmarking in der *SIEM* Landschaft

Die Chancen und ggf. Aufdeckung der Lücken bei der Implementierung der *FRs* bezüglich der *SLs*, können für ein Unternehmen evaluiert werden, indem, für jeden *security level* (SL_i), ein oder mehrere 'vertikale' (SL) Benchmarks (in Abbildung 1 Achse 'Angriffsmotivation') entworfen werden, die dann eine konkrete Aussage über die *QoS* der implementierten *foundational requirements* (*FR*) in Bezug auf den gewählten SL_i *(i=1,...4)* erlaubt.

[5] die Aktion 'correlation' ist dem sog. plan-do-check-act cycle der Normen ISO27001 ISM und ISO27044 SIEM entnommen;

Genauso können für jede FR_j *(j=1,...7)* -Maßnahme, 'horizontale' (FR) Benchmarks (in Abbildung 1 Achse 'Abwehrmaßnahmen') entworfen werden, um die Widerstandsfähigkeit (*resilience*) einer *FR*-Maßnahme gegenüber der Angriffsintensität (SL_1 *bis* SL_4) zu testen. Jede SL_i benchmark enthält k_j *CR*-Tests für jede einzelne FR_j-Maßnahme.

1. Beispiel: Für FR_1 *=IAC 'Identifikations- und Authentizitätskontrolle'* werden, mittels einem *Benchmarking*, die Resilienz-Eigenschaften allen identifizierten und authentifizierten Personen, SW-Prozessen und Geräten gegenüber evaluiert, in Bezug auf:

1. die Existenz von gelegentlichen oder zufälligen nicht-authentifizierten Entitäten (*SL1*);
2. beabsichtigtem, nicht-authentifiziertem Zugang von externen Entitäten, die einfache Hilfsmittel mit geringem Aufwand, grundsätzlichen Kenntnissen und niedriger Motivation, haben (*SL2*);
3. beabsichtigtem, nicht-authentifiziertem Zugang von externen Entitäten, die komplexe Hilfsmittel mit moderatem Aufwand, aber mit *IACS* Kenntnissen ausgestattet sind und mit moderater Motivation, vorgehen (*SL3*);
4. beabsichtigtem, nicht-authentifiziertem Zugang von externen Entitäten, die komplexe Hilfsmittel mit hohem Aufwand, und mit *IACS* Kenntnissen ausgestattet sind und mit hoher Motivation, vorgehen (*SL4*).

Ein *IACS benchmark* muss so konstruiert sein, dass er Hinweise auf Schwächen (*vulnerabilities*) und Verletzungen (*incidents*) gibt, damit sie erkannt und ausgeglichen werden können. Die Tests bzw. Benchmarks geben somit Hinweise auf Sicherheitsschwächen und -verletzungen, die in *53 Component Requirements* $CR_{j,k}$ eingeteilt werden und sozusagen die dritte Dimension 'Auswirkungen' der *SIEM-Landschaft*, darstellen, wobei *j=FR-Index* und $(k \in N)$ die Anzahl der Tests, bzw. der sog. Komponenten CR_k *je* FR_j bedeuten.

In der Abbildung 2 *'CR Benchmarking auf der SIEM Landschaft'* sind die 3 Dimensionen des Benchmarking, horizontal FR_j *(j=1,...7),* vertikal SL_i *(i=1,...4)* und tief $CR_{j\,k}$ $(k \in N)$ anschaulich dargestellt. Die Basis (FR_j*$CR_{j,k}$) besteht aus dem Kreuzprodukt aus den Abwehrmaßnahmen (7 *foundational requirements* FR_j) und den entsprechenden Testfällen (53 Component Requirements $CR_{j,k}$) und bildet die *SIEM-Landschaft* eines IACSystems, spezifisch für jedes *KMU*; d.h. ein *KMU* das ein Sicherheits-*benchmarking* benötigt, wählt aus der *SIEM-Landschaft* die zu überprüfenden Systemfunktionen aus und auf welchem Sicherheits-Level zu testen ist. In der Abbildung 1 sind das die, vom KMU eingetragenen, (grünen) Blöcke. Das daraus abgeleitete spezifische *benchmarking* umfasst Tests für alle Blöcke auf dem angegebenen Sicherheits-Level. Um die Anwendung der *SIEM-Landschaft* zu demonstrieren, wurde FR_6*=TRE* mit genau 2 $CR_{6,k=1,2}$ ausgewählt:

2. Beispiel: $FR_6 \cdot CR_{6,(k=1,2)} \cdot SL_2$ *benchmarking*: Die Basis dieses *Use Case* bildet das Produkt aus *'foundations requirements_timely response to an event'* (FR_6 *=TRE)* · *'accessibilty and monitoring tests'* $CR_{6,(k=1,2)}$ auf der spezifischen Sicherheitsstufe *'Mittel und Ressourcen eines gering motivierten Angreifers'* (SL_2).

Mit der Auswahl von FR_6*=TRE* (im Beispiel) werden auch geeignete *component requirements* ($CR_{6.k}$ *, k=1,2),* d.h. Maßnahmen, bzw. Tests festgelegt:

- $CR_{6.1}$: Durchführung von Audits über Zugangs- und Zutritts-Optionen von autorisierten Personen, SW-Prozessen oder -Werkzeugen und die periodische Lieferung von forensischen Beweisen ohne Anfragen;
- $CR_{6.2}$: Qualitätsprüfung des kontinuierlichen Monitorings von *IACS* Komponenten. *IACS* Monitoring kann erfolgen, indem Techniken, wie *IDS/IPS*, Schutz vor Schad-Software,

Netzwerküberwachung, eingesetzt werden. Für höhere Sicherheitsstufen müssen diese einfachen Techniken ebenfalls höheren Anforderungen genügen, z.B. ein einfaches *IDS/IPS* für *SL2*, wird auf ein verhaltens-sensibles *IDS/IPS für >SL2*, aufgerüstet.

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 Untersuchungen 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.

Die Empfehlungen *IEC 62443-4-2* [IEC15] beinhalten 53 Spezifikationen von $CR_{j,k}$ -test cases, wobei $CR_{j,k}$ $k \in N$, *7* Listen der *IACS*-Komponenten der Länge k_j darstellen und die Basis $FR_j \cdot CR_{i,k}$, mit jeweils k_j Sicherheitsmaßnahmen bildet. Wenn man zu dieser Basis die dritte Dimension der Sicherheits-Level *SL1 bis SL4* hinzunimmt, entsteht eine 3-dimensionale Landschaft, mit $(j \cdot k_j)$ 'Bauklötzchen' der SL-Höhe $i=1,...4$.

In Ergänzung zur sog. *SIEM-Landschaft* (bezeichnet die Basis in der Abbildung 2) 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 dieses Vorhabens), genannt wird.

In der Tat, spricht u.a. der Technische Report WD 19608:2015-07-15 [ISIE15] 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.

Ein *C-Slang* braucht Ausdruckskraft, um kritische Sicherheitsvorfälle in der *SIEM* Landschaft hinreichend ausformulieren zu können. Z.B. hat die *[ETSI ISG ISI]* alle Sicherheitsvorfälle in sog. Indikatorklassen: *'Incidents (Ixx), Vulnerabilties (Vxx) und Impacts (IMP)'* eingeteilt.

Die vollständige Spezifikation der 7 *IACS*-Operationsfelder mit jeweils k_j Komponenten (vgl. 7 lists of *CR-benchmarks*), welche die Basis der SIEM-Landschaft bildet (s. Abbildung 2), sind vorläufig nicht Teil dieses Vorhabens, werden aber in nachfolgenden 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

[ETSI01] ETSI GS ISI 001-1/2 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“

[ETSI02] ETSI GS ISI 002 Information Security Indicators (ISI) – Security Event Model (SEM) „A Security Event Classification Model and Taxonomy“

[IEC15] 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://web-store.iec.ch/preview/info_iec62443-2-4%7Bed1.0%7Db.pdf

[ISIE15] 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

[MeRR15] J. deMeer ssl.eu GmbH, Axel Rennoch FhG-FOKUS, Jens Richter, ssl.eu GmbH, "Mehr Datenschutz und Betriebssicherheit durch Cyber Security Testing", ASQF SQ Magazin Ausgabe 34, März 2015, S.28-31

[WDGX15] 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

[BSI12] 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

[IECN15] 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

[BMBF13] Acatech, Forschungsunion: Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 – Abschlussbericht des AK Industrie4.0, BMBF April 2013

[BSIC12] BSI Empfehlung: IT in der Produktion - Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen; BSI-CS10 | Version 1.00, 29.5.2012

[Adol15] P. Adolphs: RAMI4.0 – An Architectural Model for Industrie4.0, DIN Berlin, 18.6.2015

[Hoff15] Michael Hoffmeister, Festo AG&Co.KG: ZVEI The Industrie4.0 Component, Version 1.0 April 2015

[Meer14] J. deMeer, smartspacelab.eu GmbH Berlin: Dynamische Kritikalitätsbewertung von Prozessen in Kritischen Infrastrukturen, GI/ACM RG BB White Paper 3.2.2014, ONLINE: linkedin.

[BMWE16] BM f. Wirtschaft und Energie: IT-Sicherheit für die Industrie4.0; Abschlussbericht zur Studie im Auftrag des BMWE, Januar 2016.