Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 1001

On Industry4.0 Security, Maturity and Metrics semantically integrated by a Common SIEM Specification Language

Jan de Meer[1] und Jochen Link[2]

Abstract: Für die Festlegung eines zu erreichenden Sicherheitslevel SL-Target für Industrielle Produktionsanlagen IACS sind ihre Einsatzbedingungen maßgebend. Im Rahmen der Lebenszyklus-Definition (s. IEC 62443-4-1), muß u.a. ein Risk Assessment (s. IEC 62443-3-2 [IEC15c]) durchgeführt werden. Das Risk Assessment bezieht sich auf das gesamte System und auf einzelne Komponenten. Für die betrachteten Komponenten sind die IT-Gefährdungen zu überprüfen und ggf. Maßnahmen abzuleiten. Gegenstand von Sicherheitsüberlegungen von Industrieanlagen sind Fragen, welche Maßnahmen zu ergreifen sind, die sich z.B. aus dem vorgenannten Risk Assessment ergeben. Zur Modellierung und eindeutigen Darstellung soll eine gemeinsame 'SIEM Sprache' gefunden werden, die einerseits, in Ergänzung zu STIX/CybOX™ für das Management von Sicherheitsobjekten, die in XML (s. CybOX Object Listing) dargestellt werden und die andererseits für das Management von beobachtbaren Ereignissen mit signifikanten Sicherheitsinformationen (SIEM), auf Grundlage einer operationalen Semantik, geeignet ist. Aus diesem Ansatz ergibt sich, u.a. um verschiedenartige Werkzeuge integrieren zu können, eine universelle SIEM Kommunikations-Schnittstelle, an welcher Sicherheitsereignisse asynchron, mittels einer publish-subscribe SIEM middleware, als auch Sicherheitsobjekte, wie in der CybOX Liste spezifiziert, jedoch inform von <n-tuples> im sog. <n-tuple> space (vgl. JavaSpaces, SQLSpaces etc.), ausgetauscht, bzw. gemanagt werden. Dieser Beitrag zielt darauf ab, eine sog. SIEM Landschaft, bzw. eine universelle Schnittstelle für den Austausch von standardisierten Sicherheitsereignissen, im Format sog. <n-tuples>, aufbauend auf den standardisieren Konzepten 'Maturität - Indikatoren - Metriken', weitgehend formal, in operationaler Semantik, zu entwerfen.

Keywords: SIEM middleware, Information Security Indicators, <tuple>space, STIX/CybOX™, Industry4.0, IACS, ADT-based specification, Graph Manipulation Tool, Operational Semantics

1 Vermessung der Sicherheit in IAC Systemen

In [SLAMM16][3] ist eine 'Metrik' definiert, als 'Standardisierung der (Ver-)Messung einer Systemeigenschaft (Charakteristikum)' mit den Parametern: Berechnungsregel, Meßeinheiten, Anwendungsregeln, sonstige Parameter. D.h. die Metrik liefert Kenntnisse über die zu vermessende Systemeigenschaft, inbezug auf Wiederholbarkeit,

[1] Club R2GS German Chapter c/o smartspacelab.eu GmbH Berlin, Berner Str. 21B, 12205 Berlin, demeer@smartspacelab.de
[2] Ing. Link Ingenieurbüro, Spraulauche 14, 68782 Brühl, jlink@ing-link.de
[3] Das Normungsdokument ISO/IEC 2nd CD 19086-2 beschreibt die Metriken für *Cloud Computing* Dienste; nach Meinung der Autoren dieses Aufsatzes ist die Definition für Metriken auch für Industrie-Anlagen anwendbar, weil sie im Normenentwurf CD19086-2 sehr grundsätzlich ausfällt.

doi:10.18420/in2017_102

Reproduzierbarkeit, Vergleichbarkeit und grundsätzlich mögliche Meßergebnisse.

In einem Entity Relationship Diagramm (Abb. 2 in [SLAMM16]), wird die Vermessung einer Systemeigenschaft (measurement) durch eine spezifische Metrik (metric) definiert. Die Vermessung wiederum liefert Meßergebnisse (measurement results); wodurch die Systemeigenschaft (property) quantitativ eingeschätzt werden können. Die Meßergebnisse liefern somit Erkenntnisse (knowledge) über die vermessenen Systemeigenschaften.

Im folgenden Abschnitt werden die wichtigsten Begriffe, wie sie in CSlang Verwendung finden, definiert:

Metriken sind die geforderten Invarianten in einer Industrieanlage, die, wenn sie sich dennoch ändern, anzeigen, daß in der Anlage, bzw. im System, Maßnahmen geschehen sind, die eine bestimmte Metrik, z.B. den vorgeschriebenen Sicherheitsstandard, verletzen.

Indikatoren sind die zu vermessenden veränderlichen Parameter der Metrik, z.B. die verschiedenen Krümmungsparameter einer gebogenen Fläche mit unveränderlichem Inhalt (Metrik), die Hinweise darauf geben können, ob ein gegebener Sicherheitsstandard, bzw. -metrik, eingehalten worden ist oder nicht.

Gradienten stützen sich auf kontinuierliche Vermessung der Indikatoren einer Metrik. Im Beispiel des Vorgangs des Verbiegens von Flächen bedeutet das, daß in jedem Augenblick der Gradient, d.h. das Differential der Verbiegung und das Flächenmaß, bzgl. der spezifizierten Flächenmetrik, berechnet werden kann. Sicherheitstechnisch könnte der Gradient dafür genutzt werden, die Veränderungen zu berechnen, die ein Eindringversuch in ein, mit entsprechenden Indikatoren versehenem System, bewirken.

SIEM <n-tuple> space, auch SIEM Kanal oder SIEM Plattform genant, stellt die universelle Kommunikation zwischen Prozessen in kombinierten ICT- und IAC-Systemen dar und entspricht dem antizipierten SIEM aus dem ehemaligen Normungsvorhaben 27044.5[SIEMb15]. Ein <n-tuple> hat eine duale Natur, er ist einerseits ein Abstrakter Datentyp (ADT) der Daten und Attribute enthält und andererseits ein (Sicherheits-) Ereignis, das von Systemprozessen erzeugt und in den <n-uple>space gelegt wird. Der <n-tuple>space, der identisch ist mit SIEM, vermittelt die Sicherheitsereignisse zwischen den kommunizierenden Prozessen, technisch wie eine publish-subscribe middleware.

Maturity Levels (ML) beschreiben die Prozessfähigkeit (process capability) entsprechend [DIN ISO/IEC 15504-1:2011], d.h. die Fähigkeit eines Prozesses, aktuelle oder künftige Geschäftsziele zu erreichen. (Anmerkung: Der Begriff des Maturity Level (Reifegrad) nach dem Capability Maturity Model Integration (CMMI) Konzept, ist nach dem letzten Entwurf IEC 62443-3-3:2015[IEC15a] noch nicht hinreichend definiert.)

IACS[4] Referenz Architekturmodell (RAM) in Abbildung 1 beinhaltet die wesentlichen IACS Domänen, bzw. Komponenten:

- Sensoren und Aktoren im Feldbereich, verbunden über einen Feldbus;
- die Steurung der Feldkomponenten wird von einem Netzwerk (Distributed Control Network) von PLCs (Programmable Logical Controllers) ausgeführt;
- In separaten IACS Anlagen befinden sich darüber die Management Komponenten des Enterprise Resource Planning (ERP) und das Manufacturing Execution System (MES);
- eine zusätzliche I4.0 Plattform [s.a. VDE ETZ SPEC] liefert die Interkonnektivität zwischen verteilten IACS eines globalen Unternehmens, mit den Plattformkomponenten:
  - IoT[5] Gateway für die Interkonnektivität zwischen verteilten und lokalen IACS Applikations Servern;
  - SCADA[6] Monitoring und Display Warte des SOC eines lokalen IACS;

Komponentenweise Darstellung IACS Referenz-Architektur-Modell:

[4] IACS, Abkürzung für 'Industrial Automation and Control Systems', und 'Smart Factory' werden bei der Betrachtung einer IRAM, bzgl. des Normenentwurfs [DIN NA043-01-41AA N0764] als synonyme Begriffe verwendet;

[5] IoT, Abkürzung für 'Internet of Things' der Normungsgruppe ISO/IEC JTC1 WG11, bzw. DIN NA043-01-41;

[6] SCADA, Abkürzung für 'Supervisory Control and Data Acquistion', beinhaltet Komponenten zur IAC System Daten Erhebung und zur Echtzeitanalyse der unterliegenden Control NW Domains;

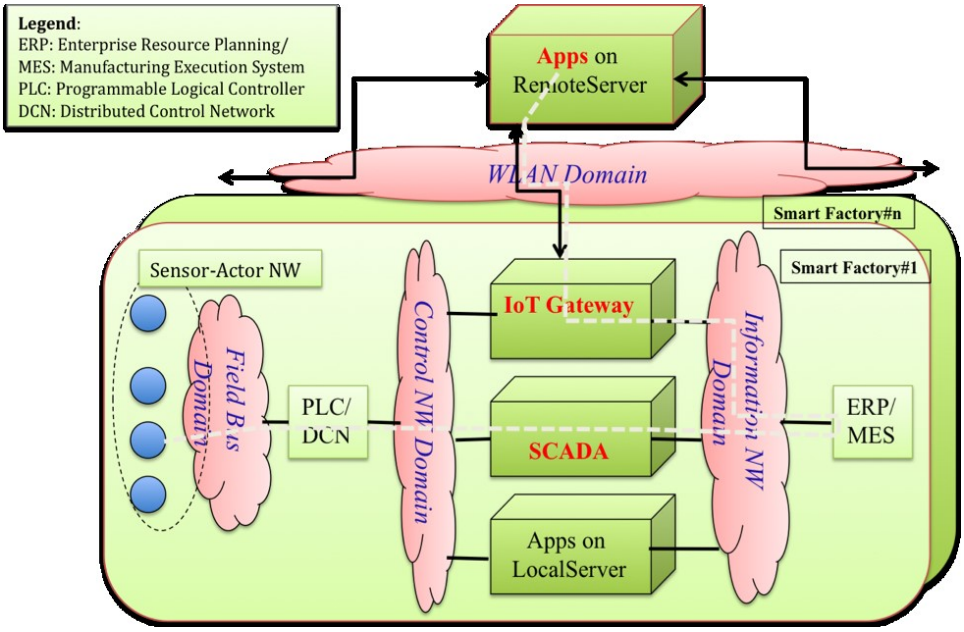

Abb. 1: IACS Referenz-Architektur-Modell

2 Umsetzung Security und Process Maturity Levels

Im Normenentwurf IEC 62443-3-3:2013[IEC15a] Security for IACS part3-3: System Security Requirements and Security Levels werden folgende drei Security Levels (SL) definiert: 1) der Target SL (SL-T) steht für die zu erreichende bzw. gewünschte Sicherheitsstufe eines Systems; 2) der Achieved SL (SL-A) steht für den erreichten SL bzw. den realisierten SL im Betrieb eines Systems; und 3) der Capability SL (SL-C) steht für den erreichbaren SL, den Komponenten oder Systeme bei richtiger Konfiguration und Integration ohne zusätzliche Maßnahmen liefern.

Die IACS Prozessfähigkeit bzgl. eines bestimmten Maturity Level wird z.B. nach dem Konzept Capability Maturity Model Integration (CMMI) [HeKn11], in die Klassen (ML) 1 bis 5, eingeteilt.

Maturity Levels werden in ähnlicher Weise, im Umfeld von Smart Cities verwendet; dazu die folgende Anmerkung: Mit [SCMM16] gibt es seit 2015 ein neues Normungsprojekt "Community Infrastructure Maturity Model (CIMM)" der Arbeitsgruppe JTC1 WG11 Smart Cities (das heute bereits den CD-Norm-Maturity Status erreicht hat). Mit "Community" sind hier die, für notwendige Investitionen in städtische, wie ländliche Infrastrukturen (Energie, Wasser, Verkehr zur Schiene, Straße,

Luft und Industrie-Anlagen, ICT/Cloud Server etc.), verantwortlichen Gemeinden gemeint.

Zu Beginn eines neuen Vorhabens werden die Anforderungen an die System Komponenten und Sicherheitsmaßnahmen, entsprechend [JLi16] und [JLi14] festgelegt. Die Ausgangsbasis dafür ergibt sich aus den gesetzlichen Grundlagen für das Data Management für die Sicherheitsbereiche IT Safety und Technische Anlagen.

Je nach Anforderung an eine Komponente und dem zugeordneten Security Level (SL, siehe Abschnitt 3) wird die vorhandene IT Infrastruktur in Zonen untergliedert. Zonen mit niedrigem SL1 müssen weniger Anforderungen erfüllen, als eine Zone mit SL4. Die Security Anforderungen an den Datenaustausch an Schnittstellen, sog. Conduits hängen von dem gewählten Security Level ab. Wenn im Extremfall alle Komponenten in einer einzigen Zone zusammen gefasst werden, gilt der Security Level für die am höchsten eingestuften Komponenten für alle Komponenten.

Für jede Entwicklung im Rahmen der IEC 62443 ist eine Risikobeurteilung (Risk Assessment) erforderlich. Wie sich diese Risikobeurteilung mit dem übergeordneten Risikomanagement für ein Unternehmen (ISO 31000), mit Vorgehensweisen zu ISO 27003 / 27005 und bezüglich der technischen IT Security (IEC 62443), mit Safety (IEC 61598-1) etc. abstimmen läßt, wird in Abbildung 4 mit folgender schrittweisen Vorgehensweise [JLi14], [JLi16] beschrieben:

Schritt 1: definiere interne und externe Kontexte, *Scope* und Anwendungsgebiete;

Schritt 2: identifiziere Projektziele und Begrenzungen (*Boundaries*) des betrachteten *IACS*:
IEC 62443-3-2 Abschnitt 4.1 und IEC 61508-1 Abschnitt 7.3;

Schritt 3: führe *High Level Risk Assessment* durch:
IEC 62443-3-2 Abschnitt 4.2;

Schritt 4: definiere *Security* Anforderungen:
IEC 62443-3-2 Abschnitt 4.3;

Schritt 5: spezifiziere Komponenten, Zonen, Verbindungen *(Conduits)*:
IEC 62443-3-2 Abschnitt 4.4, detaillierte Angaben in IEC 62443-4-1 Abschnitt 7;

Schritt 6: führe detaillierte Risikoabschätzung durch:
IEC 62443-3-2 Abschnitt 4.5 und bezüglich Security siehe ISO 12100;

Schritt 7: entwerfe Gegenmaßnahmen bzgl. festgestellter *Security* Schwachstellen;

Schritt 8: führe zyklische Aktionen aus: Monitoring -> Revision -> *IACS* Betrieb;

Schritt 9: dokumentiere den gesamten *Risk* Management Prozeß:

Abb. 4: IACS Risikoabschätzung, gestützt auf Normen ISO 31000, ISO 270 03/05, IEC62443-3-2, IEC62443-4-1, Lifecycle aus IEC61508-1.

Bei der Risikoabschätzung (s. Abbildung 4) sind für die Systemkomponenten die jeweiligen Gefährdungen, z.B. sog. Hazards, zu ermitteln. Ein praktisches Beispiel einer Bedrohungsmatrix für eine Switch Komponente in Abbildung 2, wird in Abschnitt 4 formal spezifiziert und in Abbildung 3 als ADT vorgestellt.

Aus dem Umfeld der (Office) IT Sicherheit ist das Management System der ISO 27001 bekannt. Etwas ähnliches wird es im Rahmen der IEC 62443-2-1 für den technischen Anwendungsbereich bzw. für IACS geben.

In Ergänzung zu Abbildung 4 zur Risikobeurteilung soll die Norm ISO 31000 ebenso betrachtet werden. Damit wird die Verbindung zum integrierten Management-System bzgl. der Risikobeurteilung hergestellt. Die Integration der Maßnahmen zur IT Security aus dem technischen Umfeld in ein integriertes Management-System ist möglich. Die High Level Struktur von Management-Systemen besteht aus den Maßnahmen, bzw. Aktionen: plan-do-check-act in zyklischer Art und Weise.

Die IEC62443-2-4 beschreibt die Anforderungen an das IT-Sicherheitsprogramm für Dienstleister. Die Anforderungen beinhalten beispielsweise die Themen: Mitarbeiter,

Systemaufbau, Verwaltung von Nutzerkonten, Datenübertragung, Konfigurationsverwaltung, Behandlung von Ereignissen, Schutz gegen Schadsoftware, Patch Management und Datensicherung bzw. Wiederherstellung.

Funktion, Dienst, Zugriff	**Bedrohung**	**Schwachstelle**	**Folge**	**Maßnahme**
Physischer Zugriff (Sicherheit)	direkter Zugriff, offene Ports, Manipulation Kabel	Kein Zugriffsschutz	Zerstörung oder Manipulation	Zugriff beschränken, geschütztes Umfeld
Port Sicherheit	Netzwerkzugang über Firewall hinweg	Schlechte Konfiguration, Zugang Anschlußdosen	Manipulation, keine Verfügbarkeit, Informationsbeschaffung	Netzwerkzugang einschränken, Organisation Zuständigkeit
Einfluss auf Datenverkehrs-Steuerung	DoS Angriff, Netzüberlastung mit Nachrichten	Zeitlicher Anforderungen an Automatisierung, Konfiguration	Zeitliche Kommunikationsanforderungen werden nicht erfüllt	Einsatz managebare Switche, Absicherung Bandbreite
Access Conrol List (ACL)	Unkontrollierte Nachrichtenströme	Mangel Kontrolle n Nachrichtenströme	Mangel Kontrolle	Einsatz von ACL, Maßnahmen abhängig vom Switch
Quality of Service (QOS), Rate Limiting	Hohes Datenaufkommen, Auslastung bestimmen	unzureichende QoS Klasse	Bedarf an Bandbreite berechnen	für verändertes Datenaufkommen geeignete Verkehrsklasse wählen; Weiterleitung nach Priorität;
Dynamic ARP Inspection [NWL15], [CIS17]	ARP Spoofing Attacken (Anfrageverfälschung)	ARP Spoofing	Manipulation Datenverkehr zw. Netzwerktei-lnehmern	ARP Inspection umsetzen, prüfen durch Switch ob IP, MAC Adressen u. ARP Antworten passen
IP Source Guarding	Bei IP Spoofing – IP Pakete mit gefälschten Absenderadressen	Zielsystem kann nicht erkennen von welchem Absender Pakete kommen	Nicht erwünschte Weiterleitung von Paketen	Switch pflegt mit DHCP Snooping eine Tabelle mit VLAN ID, IP u.MAC Adresse angeschlossener Systeme, nicht passende Pakete werden verworfen
CAM Flooding Protection	Switch kann sich keine Port / MAC Adressen mehr merken	Switch leitet Pakete an unbekannte MAC Adressen	Man-in-the-Middle Angriffe, Abhören von Daten	Content Addressable Memory (CAM) Flooding Protection umsetzen

Abb. 2: tabellarische Darstellung Bedrohungsmatrix für eine Switch Komponente.

3 Sicherheits-Indikatoren und Metriken

Sicherheitsstufen SL1 bis SL4, inbezug zu 'Foundational Requirements (FR)' entnommen der Normen IEC 62443-3-2 und angewendet auf industrielle Infrastrukturen [MeWa16] zeigen, daß in einem bestimmten Maßnahmenbereich, z.B. 'zeitgerechte Reaktionen auf sicherheitsrelevante Ereignisse' (FR_6=TRE) in industriellen Automatisierungs- und Kontrollanlagen (IACS), auch auf der niedrigen Sicherheitsstufe SL2:= 'geringe Motivation der Angreifer', erwartet werden können. Um wenigstens diese geringe Sicherheitsstufe sicherzustellen, werden geeignete Indikatoren benötigt, die Ereignisse von IACS-Maßnahmen über einen bestimmten Zeitraum "anzeigen" (monitoring) und ggf. über alle beobachteten Verstöße (incidents) gegenüber spezifizierten Sicherheitsanforderungen, Meldung geben und Beweise für nachfolgende forensischen Untersuchengen, sicherstellen.

In [ReGa16] ist eine kategorisierte Darstellung in der 'ETSI Information Security Indicators (ISI)' Tabelle [ETSI01] enthalten, was in einem Beispiel für 'Malware' Indikatoren verdeutlicht werden soll:

1. Malware bildet eine (family: MLW), die der (class: IEX) für 'Intrusions and External Attacks' angehört. Die Familie MLW besteht aus 4 ISI Komponentenbeschreibungen;
2. Für jede ISI-Beschreibung (Komponente) gibt es eine geeignete ISI-Spezifikation, bestehend aus den Parameter-Spezifikationen und Erwartungswert-Spezifikationen:

Die notwendigen Angaben zur Vermessung der Indikatoren, Parameter und Erwartungswerte, bestehen jeweils aus einem <tuple>-Element <spec wert>. Alle <n-tuples> ob einzeln oder in Kombination, werden im <n-tuples>-space als SIEM Ereignisse gemanagt (s. Abschnitt 'Operationale Semantik').

4 Operationale Semantik der Sicherheit

Die antizipierte Semantik des formalen Teils der Beschreibungssprache CSlang ist ein sog. Abstrakter Datentyp (ADT), der auf Grundlagen algebraischer Ansätze formaler Sprachen, gebildet wird und aus [BoMo79], [EhMa85], [Mos04] u.a. entlehnt ist.

ADTs können verglichen werden mit dem Ansatz 'Objekt-orientierter Entwurf (OO Design)'. Jeder ADT, bzw. Objekt besteht aus Datenmengen, SORTS, und Beziehungen zwischen diesen Datenmengen, OPNS (Operations), genannt. Ergänzt man Sorten und Operationen mit Regeln RULES (auch EQNS) genannt, so erhält man semantisch eine Algebra (vgl. Boolesche Algebra mit der einzigen Sorte BINARY, den konstanten Ziffern W und F, den 1- und 2-stelligen Operationen NICHT, UND, ODER, IMPLIKATION, den Regeln für Distributivität, Assoziativität, Kommutativität,

Idempotenz etc. und ggf. weiteren abgeleiteten Regeln, wie de Morgan, Komplement, Absorption etc.). Mittels der Regeln werden reguläre Ausdrücke gebildet, die Repräsentanten von {W, F} in der Sorte BINARY sind. Es entstehen also Objekte mit algebraischer Semantik, d.h. Abstrakte Datentypen (ADTs).

Ein ADT kann in CSlang u.a. auch als Prozeß fungieren. Prozesse akzeptieren Eingaben und produzieren Ausgaben, in asynchroner Art und Weise, bedingt durch die geforderte Autonomie der Prozesse. Daher sind Ein- und Ausgaben **Ereignisse**, die das Verhalten der Prozesse bestimmen: Prozesse konsumieren (konkrete) Ereignisse subskribierter Ereignisdatentypen und publizieren (konkrete) Ereignis bestimmter Ereignisdatentypen. Ereignisse als auch Daten werden also algebraisch typisiert, d.h. es entsteht ein 'multisorted ADT'. Die 'Ereignis ADTs' werden als <n-tuples> mit n Ereignis-Attributen <spec value>, dargestellt und werden somit im <tuples>space publiziert und konsumiert.

Als ADT Spezifikations-Beispiel soll eine ' Bedrohungsmatrix' für eine Switch Komponente (s. Abbildung 2: tabellarische Darstellung und Abbildung 3: ADT Darstellung einer 'Bedrohungsmatrix'), als 8 mal <5-tuple>, also eine Matrix mit 8 Zeilen mit je 5 Einträgen, formal spezifiziert werden. Das Ergebnis ist in der Spezifikation 'ADT Bedrohungsmatrix' in CSlang enthalten (s. Abbildung 3):

Zunächst werden für die Anwendung 'Bedrohungsmatrix' die benötigten 5 Datentypen (alg. Sorten) angegeben:

```
SORTS: TupleSpace Function Threat Vulnerability Impact
Measure;
```

wobei TupleSpace eine Ergebnissorte ist, die alle generierten <5-tuples>, also den Wortschatz einer Anwendung im TupleSpace, enthält.

Eine mögliche Bedrohung, z.B. die 5 Matrixzeile, als <5-tuple> lautet:

```
<QoS BwOccupied BwAnticipated QoSControl GuardQoS>;
```

wobei die <5-tuple> Elemente Datentypen, mit einem bestimmten Definitionsbereich sind.

Wie in Abschnitt 3 erläutert, kann jeder <n-tuple>Eintrag einen Wert aus seinem spezifischen Definitionsbereich annehmen; z.B. kann der obige Bedrohungs<tuple> mit seinen 5 Spezifikationen ergänzt werden, durch entsprechende Werte, die eine mögliche QoS-Bedrohung quantifizieren und ggf. korrigieren können[7]:

```
<'qosClassX' '90%' '60%' 'bandwidth(X-Y)'
'changeQoSClassY'>;
```

[7] der einfachheithalber werden an dieser Stelle <*tuple*> Spezifikation und -Werte nur korrespondierend und nicht paarweise, d.h. <*spec wert*> angegeben.

Diese Werte stellen sozusagen die Kurzform eines Programms, bzw. eines Regulierungszyklus, dar, das beschreibt, was geschehen muß, um den gemessenen QoS-Engpaß zu vermeiden, bzw. zu korrigieren; z.B. könnte ein Überschuß an nicht benötigter Bandbreite anderweitig verwendet werden.

ADT Spezifikation einer 'Bedrohungsmatrix' (Zeile 5 aus tabellarischer Darstellung in Abbildung 2):

```
ADT:  Threat Matrice {
      BASIC: Bool Int;
      SORTS: TupleSpace Function Threat Vulnerability
             Impact Measure;

      OPNS: <..> --> TupleSpace;

      OPNS: PhysAccess PortSecurity TrafficControl
            ACL QoS DAI IPSrcGuard CAM-->Function;

      OPNS: Access2Devices Access2NW DoS
            UncontrolledDFlows BwOccupied DAISpoofing
            IPSpoofing CAMFlooding-->Threat;

      OPNS: DeviceAccess NWConfiguration
            TimeConstraint DFlowControl
            BwAnticipated ARP IP CAM-->Vulnerability;

      OPNS: DeviceManipulation Availability
            TimeWindow DFlowControl QoSControl
            ARPManipulation IPManipulation MiMAttack
            -->Impact;

      OPNS: GuardDeviceAccess GuardNWAccess
            GuardSwitchBandwidth GuardACL GuardQoS
            GuardARP GuardIP GuardCAM-->Measure;

      RULES: select{
                  +Function:QoS∃QosClassDef
                  +Threat:BwOccupied∃BwRatio
                  +Vulnerability:BwAnticipated∃BwRatio
                  +Impact:QoSControl∃BwInteger
                  +Measure:QoSGuard∃BwSignal
                   } == <FTVIM valuetuple>;
...}
```

Abb. 3: ADT Darstellung einer Bedrohungsmatrix für eine Switch Komponente

5 Ergebnisse und Ausblicke der Industriellen Anwendung

Während die Datennetze den Datentransport auf der Grundlage von Kommunikationsprotokollen, in großer Menge auf großen Distanzen zwischen vielen Stationen bewältigen, bewältigen die IACS Anlagen dedizierte anlagen-stringente Meßdaten von der Sensorik zur Anlagen-, bzw. zur Fabrikkontrollstation (s. Abbildung 1), der sog. 'Security Operation Control Center' (SOC), die anschließend eine Analyse der publizierten Meßdaten, inform von Ereignis<tuples> vornimmt und daraus die Signale zur Steuerung der Anlage, bzw. Fabrik analysiert, berechnet und für die Anlagenaktoren publiziert. Jeder Aktor entspricht einem Ereignistyp, den er subskribiert hat. So entsteht ein Kontroll- und Regelkreis auf Grundlage einer formalen SIEM Plattform für IAC Systeme. Die SIEM Plattform ist integrales Kommunikationsmodell des umfassenden formalen CSlang Modells für Informations-Sicherheits-Indikatoren (ISI, [ETSI06]), wie vorangehend vorgestellt.

Alle angemeldeten Komponenten (subscriber role) bei der SIEM Plattform, wie Prozesse, Sensoren, Aktoren, Kontrollstationen, Produktionsprozesse (s. Abbildung 1) eines IAC Systems, werden sofort auf die Ankunft eines neuen Ereignis<tuples> hin informiert und können es konsumieren, verarbeiten und ihrerseits Ereignis<tuples> generieren und publizieren (publisher role), also neue Datenformate in den SIEM<tuples>space stellen. Eine Komponente kann also beide Rollen, subsrciber und publishcr Rolle, gleichzeitig spielen. Eine subscriber Komponente braucht nur die interessierenden Ereignis<tuple>Datentypen zu abonnieren. Die Verwaltung der Ereignis<tuples> übernimmt die SIEM Plattform bzw. der SIEM Kanal.

Nun ist es so, daß aufgrund der Digitalisierung, einzelne Komponenten, wie z.B. die Anlagenkontrollstation SOC, wie in Abbildung 1, ausgelagert werden könnte, wie es die 'Industrie4.0 Plattform' (s. VDE ETZ Dokument [DIN NA043-01-41AA N0764]) zwar vorsieht, jedoch im CSlang Modell, nur im Format eines <tuples>space, geschehen kann. Ein großes Industrie-Unternehmen könnte entscheiden, daß die Anlagenkontrolle, z.B. in der Autoindustrie, von einem zentralen Server aus, vorgenommen wird. Dazu benötigt man lediglich eine allgemeine digitale Schnittstelle zwischen den einzelnen Anlagen, ein Gateway etwa, das über das 'Internetz' (ICT) die lokalen Anlagen mit dem zentralen Server verbindet. Und schon hat das globale Unternehmen Zugriff auf die örtlichen Anlagensteuerung. Die notwendigen Daten werden dezentral erhoben und zentral verarbeitet, was eine Herausforderung für 'Security & Privacy' für das Management in globalen Unternehmen darstellt.

CSlang hält dafür ein werkzeuggestütztes Simulationsmodell, auf der Basis von Graph-Manipulationswerkzeugen z.B. GraGra der TUB [AGG17] und GrGen.NET des KIT IPD [GrGen10], bereit. Darin werden Informationen in einem IACS als Graph dargestellt. Der modellierte Graph repräsentiert also einen bestimmten IACS Zustand. Eine Zustandsänderung bedeutet eine Veränderungen der Informationen über die Komponenten eines IAC Systems, z.B. kann sich, in einem Energieversorgungsnetzwerk, bei Veränderung des Wetters (mit Indikatoren für Wind,

Sonneneinstrahlung, Tageszeit etc.) auch die Konfiguration (Zustand) der Energieerzeugungskomponenten verändern, sie können hinzu oder abgeschaltet werden. Die Informationen sind ADTs die als Ereignis<tuples> dem SIEM Kanal entnommen werden.

Der CSlang Ansatz ist semiformal, weil er das Modell einer ereignisorientierten, technischen Kommunikationsplattform (SIEM) mit formalen Ansätzen wie algebraische ADT [Mos04], [EhMa84] und Graph Theorien [AGG17], [GrGen10] etc. miteinander kombiniert. Damit erübrigt sich der Zwang zu einer vollständige Formalisierung eines zu analysierenden IACS und Designer und Betreiber können sich auf wesentliche Fragen, wie z.B. auf eine vorausschauende Simulation der Folgen einer Konfigurationsveränderung in komplexen, Systemen konzentrieren.

Weiterhin können die gerade in der Normung weitverbreiteten Tabellen zur Beschreibung von Maßnahmen oder Systemeigenschaften sehr gut mittels ADTs formal dargestellt werden. Ein ADT ist sozusagen die semantische Hülle für ein <n-tuple> im technischen SIEM Kanal.

Im Rahmen eines Normungsprojektes einer Industriellen Spezifikationsgruppe für Sicherheitsindikatoren (ISG ISI) [ETSI06] u.a. ausgeführt im Rahmen der Industriellen Vereinigung Club R2GS EU [R2GS] mit Sitz in Paris, ist es das erklärte Ziel, mit interessierten industriellen Partnern einen CSlang Prototypen, gestützt auf graphverarbeitende semantische Werkzeuge und Abstrakten Datentypen, zu realisieren und in der Standardisierung von IT/Cyber Security anzuwenden und damit zu simulierbaren, bzw. validierbaren Aussagen und Richtlinien in der Normung zu gelangen.

Literaturverzeichnis

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

[AGG17] The Attributed Graph Grammar Werkzeug, Version 2.1(2017) der TU Berlin: http://www.user.tu-berlin.de/o.runge/agg/

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

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

[BoMo79] Robert S. Boyer, J. Strother Moore: A Computational Logic, ACM Monograph Series, Editor Thomas A. Standish, UoC at Irving, Academic Press 1979

[CIS17] CISCO(2017): http://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=8

[EhMa85] H.Ehrig, B.Mahr: Fundamentals of Algebraic Specification 1/2, EATS Monographs on Theoretical Computer Science, Springer-Verlag 1985.

[ETSI01] ETSI GS ISI 001-1/2 Information Security Indicators (ISI) –

Indicators (INC) Part 1 Revision 1 FDA v0.0.3 Gerard Gaudin Rapporteur) „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“

[ETSI06] ETSI GS ISI 006 (WD v0.0.6, Jan deMeer Rapporteur) Information Security Indicators (ISI) - An ISI-compliant Measurement and Event Management Arichtecture for Cyber Security & Safety - CSlang A Cyber Security Specification Language.

[GrGen10] Karlsruhe Institut für Technologie IPD Inst. f. Programmierparadigmen: GrGen.NET Graphtransformationswerkzeug https://svn.ipd.kit.edu/trac/mx/wiki/Tools/GrGen.NET

[HeKn11] C.Hertneck, R.Kneuper: Prozesse verbessern mit *CMMI for Services*, dpunk.verlag Heidelberg 2011

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

[IEC15a] IEC 62443-3-3:2013 Security for Industrial Automation and Control Systems part3-3: System Security Requirements and Security Levels (ANSI/ISA 62443-3-3 (99.03.03))

[IEC15b] 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)

[IEC15c] IEC 2015 NP 62443-3-2 - 65/611/NP - Security for Industrial Automation and Control Systems - Part 3-2: Security Risk Assessment and System Design

[IS04-04] DIN ISO/IEC 15504-1:2004 IT Process Assessment part1 - Concepts and Vacabulary;

[IS08-15] 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

[IS07-08] ISO/IEC 12207:2008 System und Software Engineering – Software Lebenszyklus Prozesse, https://www.iso.org/standard/43447.html

[JLi16] Jochen Link Vortrag: 'IEC TC65-WG20 Management Systems and Differences - Gegenüberstellung der Grundlagen', (Folien 2-6) Okt. 2016;

[JLi14] Jochen Link Vortrag: 'Grundlagen zu Produktentwicklung, Industrie 4.0, Vernetzung und Umsetzung', (Tabellen) Dez. 2014;

[Mos04] Peter D.Mosses (Editor): CASL Reference Manual - The Complete Documentation of the Common Algebraic Specification Language, LNCS Springer Verlag 2004.

[NWL15] Networklab(2015): Dynamic Address Resolution Protocol (ARP) Inspection (DAI): http://www.nwlab.net/know-how/Cisco/dynamic-arp-inspection.html;

[ReGa16] Axel Rennoch FhG FOKUS, Gerard Gaudin ETSI ISG ISI: Information Security Indicators Quick Reference Card (updated2016-01); https://sites.google.com/site/axelrennoch/specialities/security/isiQRC.pdf https://en.wikipedia.org/wiki/Information_security_indicators

[ReGa13] Axel Rennoch FhG-FOKUS, Gerard Gaudin G^{2}C, ETSI ISG ISI: 'Security Indicators Quick Reference Card v1.1.1:2013', https://cdn1.scrivito.com/fokus/e492943d2f291a76/4905070bb7ea30262ddf855393d14e21/SQC_Download_Etsi_isiQRC1.pdf

[R2GS] http://www.net1901.org/association/CLUB-DE-REFLEXION-ET-DE-RECHERCHE-EN-GESTION-OPERATIONNELLE-DE-LA-SECURITE-CLUB-R2GS,526423.html

[SLAMM16] JTC1/SC38 N1453: 2nd CD 19086-2 IT-ClC-SLA Framework - p2 Metric Model (2016-12-06)

[SCMM16] ISO/IEC JTC1/WG11 N0156 (Convener Yicheng Zhou): CD 37153-p1/p2:2016 *Smart City Maturity Model* part 1 Introduction; part 2 Principal Contents and Project Situation;

[SCII16] JTC1 WG11 N0107 WD 30146:2016 (Convener Tangli Liu): *Smart City ICT Indicators*;

[SIEMa15] ISO/IEC JTC1 SC27 WG4 N909: ToR SP Future SIEM - Terms of Reference for a 6-month Study Period on SIEM Realignment with current developments and processes (2015-05-11)

[SIEMb15] ISO/IEC JTC1/SC27/WG4 N735 (2015-01-26) 5th WD27044 Guidelines for Security Information and Event Management (SIEM)