Safety-Anforderungen an die digitale Maschinenrepräsentanz 2020

Whitepaper SF-3.3: 09/2020

smartFactory KL®

Abstract
Die Arbeitsgruppe 2 „Connect & Control“ (vormals AG 1 „Smarte Infrastruktur“) der ***SmartFactory***^{KL} befasst sich u. a. mit dem Thema Safety in modularen Industrie 4.0-Produktionsanlagen. Für das Ermöglichen der praktischen Umsetzung einer vereinfachten, teil- oder vollautomatisierten Maschinensicherheitsbewertung sind konkrete Anforderungen an die Safety-Inhalte der digitalen Repräsentanz einer Maschine zu stellen. Im Sinne von „Plug&Produce“ und damit der einfachen Austauschbarkeit von Maschinenmodulen einer Produktionsanlage sollten die aus Safety-Sicht erforderlichen Inhalte einer digitalen Maschinenrepräsentanz standardisiert werden. Des Weiteren wurde das Erfordernis einer standardisierten Safety-Semantik erkannt. Diese beiden identifizierten Erfordernisse zur Standardisierung sind nicht nur für die Umsetzbarkeit von „Plug&Produce“ erforderlich, sondern auch für die Realisierung von „dynamischer Maschinensicherheit“, welche das Heben von zusätzlicher Effizienz und Produktivität ermöglicht.

Keywords
Safety; Industrie 4.0; automatische Zertifizierung; Verwaltungsschale

Autoren

William Motsch	Technologie-Initiative SmartFactory KL e.V.
Alexander David	Deutsches Forschungszentrum für Künstliche Intelligenz
Michael Pfeifer	TÜV SÜD Industrie Service GmbH
Dimitri Harder	TÜV SÜD Produkt Service GmbH
Josef Güntner	TÜV SÜD Industrie Service GmbH

Inhaltsverzeichnis

1. Zielsetzung des Whitepapers

Dieses Whitepaper fasst die aktuellen Ergebnisse der Arbeitsgruppe zum Thema Safety an modularen Maschinen zusammen.

In Zusammenarbeit mit den beteiligten Partnern Bosch Rexroth, B&R, Festo, Phoenix Contact, Pilz und TÜV Süd wurde zur Hannover Messe 2018 ein Konzept zur vereinfachten, teil- oder vollautomatisierten Maschinensicherheitsbewertung entwickelt und veröffentlicht [https://smartfactory.de/wp-content/uploads/2018/04/SF_WhitePaper_Safety_3-1_DE_XS.pdf]. Anhand der Beschreibung von sicheren Profilen, welche innerhalb der Verwaltungsschale (vgl. DIN SPEC 91345) definiert und abgelegt werden, konnte diesbezüglich ein Teilkonzept entwickelt werden, welches die modulare Zertifizierung von Maschinengruppen ermöglichen soll. Aufbauend auf diesen Überlegungen wurde das bestehende Konzept um mehrere Ebenen der sicherheitstechnischen Überprüfung von modularen Maschinen erweitert und zur Hannover Messe 2019 vorgestellt [https://smartfactory.de/wp-content/uploads/2019/03/Whitepaper_AG1_deutsch_042019.pdf].

Aufbauend auf den beiden vorangegangenen Whitepaper ist das Ziel dieses Whitepapers eine allgemeine jedoch eindeutige Struktur einer digitalen Safety-Repräsentanz eines Assets (Maschine oder Komponente) zu formulieren. Zusätzlich sind weitere erforderliche Schritte zu identifizieren, um die Interoperabilität zwischen der heterogenen Landschaft an Maschinen und Komponenten zu gewährleisten um daraufhin mit Smart-Safety-Agenten eine Gefährdung (bzw. das resultierende Risiko) mit einer Schutzmaßnahme gegenüberzustellen und zu bewerten. Dieses Whitepaper fasst die aktuellen Ergebnisse der Arbeitsgruppe zum Thema Safety an modularen Maschinen zusammen.

2. Einführung

Getrieben durch immer kleinere Produktionsaufträge oder der Herausforderung flexibel auf schwankende Marktanforderungen reagieren zu können, erhöht sich die Nachfrage nach modularen Anlagen und Maschinen.

Bei modularen Anlagen mit Plug & Produce Szenarien müssen Maschinen bzw. Komponenten miteinander reibungslos kommunizieren können. Handelt es sich um Komponenten bzw. modulare Maschinen von nur einem Hersteller, lässt sich die Kommunikation untereinander während der Entwicklungsphase der Anlagen berücksichtigen und die Einrichtung gestaltet sich überaus einfach, d.h. die Einrichtung und das Zusammenspiel wird in der Phase der Entwicklung / des Engineerings konzeptionell vorgedacht und der spätere Einrichtungsaufwand kann dabei vereinfacht werden. In produzierenden Umgebungen kann es jedoch erforderlich sein, dass unterschiedlichste Maschinen- bzw. Anlagentypen und damit Hersteller von Anlagen und Komponenten zusammenwirken. Insbesondere in Smart Manufacturing- bzw. I4.0-Anlagen, wo nicht absehbar ist, welche Konfiguration in der Zukunft erforderlich ist und, damit welche Maschinentypen in der Zukunft zusammenarbeiten können müssen, ist eine durchgängige herstellerübergreifende Interoperabilität erforderlich.

Modulare Anlagen müssen wie auch herkömmliche Anlagen den entsprechenden Richtlinien genügen. Sind während dem Betrieb Änderungen an der Anlage erforderlich, muss diese Änderung erneut einer Sicherheitsbewertung unterzogen werden. Insbesondere bei häufigen Änderungen summiert sich die „down time" für die erneuten Sicherheitsbewertungen, so dass bei manueller Bewertung die Vorteile einer modularen Anlage durch den Zeit- und Kostenaufwand dieser Prüfungen und Bewertungen deutlich geschmälert werden können.

Somit müssen Sicherheitsbeurteilungen von modularen Anlagen auf einer gleichen technologischen Ebene ausgeführt werden, welches es ermöglicht mit dem Austausch von Komponenten oder der Hinzunahme eines weiteren Maschinenmoduls eine entsprechende Sicherheitsbeurteilung zu berechnen und für die Freigabe mitzuteilen.

3. Digitale Repräsentanz einer Maschine

Im Zusammenhang mit der Gestaltung von modularen und wandelbaren Anlagen stößt man auf Begriffe, wie z.B. cyber-physisches Produktionssystem (CPPS), ***SmartFactory***^{KL}, Digital Twin, Internet der Dinge, digitaler Schatten uvm. Grundgedanke im Zusammenhang mit einer solchen Produktionsumgebung ist stets der Gleiche, die Vorteile digitaler Maschinenrepräsentanzen zu nutzen, um flexibler und mit einer höheren Effizienz zu produzieren.

Bezüglich der Kommunikation von modularen Anlagen und ihrer digitalen Zwillinge ist ein weiterer Begriff von Bedeutung, die Verwaltungsschale (VWS). Das Konzept der Verwaltungsschale wurde in der DIN SPEC 91345: Referenz Architektur Modell Industrie 4.0 zum ersten Mal vorgestellt. Die Verwaltungsschalle kann eine Komponente, eine ganze Anlage oder die Kombination ganzer Anlagen repräsentieren. Die Struktur der Verwaltungsschale findet sich unter anderem in der Norm IEC 62832 – Digital Factory Framework. Im Generellen beinhaltet die Verwaltungsschale einen Satz von Assets (Komponenten oder auch Maschinen) die gemeinsame Datenelemente aufweisen und von einer oder mehreren Asset Definitionen abgeleitet sind. eine VWS besteht aus einem allgemeinen Teil, in dem sich die Identifikationsinformation befindet, und kann des Weiteren aus mehreren Teilmodellen bestehen, welche spezifische Aspekte einer VWS repräsentieren, vgl. frühere Unterscheidung zwischen „Header“ und „Body“.

Im Teilmodell zu spezifischen Aspekten werden die charakteristischen Merkmale des zu betrachteten Assets abgespeichert, dies können auch Anforderungen, die einzuhalten sind, sein.

Bei der Entwicklung von modularen Komponenten oder Maschinen können gemäß DIN SPEC 91345 die charakteristischen typspezifischen Merkmale des Assets in einer so genannten Typ-Verwaltungsschale abgelegt werden.

Die Besitzer der Typ-Verwaltungsschale können diese auch nachträglich anpassen (Update), wenn eine Maschine schon auf dem Markt ist. Die Instanz-Verwaltungsschale referenziert sich auf die Typ-Verwaltungsschale. Somit werden einzelne Komponenten und Maschinen auf den neusten Stand gehalten [1]. Dies kann erforderlich werden, wenn sich bspw. durch ein Software Update der Funktionsumfang einer Komponente erweitert. Ein Update bzw. das Herunterladen und Aufspielen eines Updates einer Instanz-Verwaltungsschale einer einzelnen Komponente oder Maschinenmodul darf das Echtzeitverhalten der Maschine bzw. Anlage nicht beeinträchtigen. Die Systeme müssen weiter in der Lage sein, Alarme auszulösen und augenblicklich auf Ausfälle zu reagieren und es muss stets ein für Personen sicherer Anlagenzustand gegeben sein. Ein Aspekt, der in diesem Zusammenhang von besonderer Bedeutung ist, stellt die Cybersecurity dar.

Um die genannten Aspekte bedienen zu können und die Anforderungen der DIN SPEC 91345 6.1.6 hinsichtlich Cybersecurity und die im Folgenden näher ausgeführten Anforderungen zu erfüllen, bietet es sich an, die Normenfamilie IEC 62443, ergänzt um IEC TR 63069, zu betrachten. Dieser sogenannte „SecureSafety“ Ansatz unterstützt, dass Cybersecurity und Safety entlang des Lebenszyklus aufeinander abgestimmt wirksam sind.

Neben der Safety muss bei einem Update der Instanz-Verwaltungsschale auch stets der produzierende Betrieb einer Maschinenanlage gewährleistet sein, um die betrieblichen Anforderungen des Betreibers zu erfüllen.

Es ist somit ersichtlich, dass für die Sicherstellung der Cybersecurity Anstrengungen seitens Hersteller und Betreiber erforderlich sind. Im Rahmen der Cybersecurity-Bewertung sind nicht nur Safety-relevante Aspekte zu bewerten. Durch eine Cyberattacke soll bspw. der Betrieb der Anlage oder die Produktqualität nicht negativ beeinträchtigt werden. Diese Überlegungen stehen in diesem Whitepaper nicht im Fokus und werden nicht weiter vertieft.

Für den Betreiber einer modularen Maschinenanlage mit entsprechend digitalisierten internen Prozessen ist der Teil der Verwaltungsschale von besonderem Interesse, mit dem die Eigenschaften und aktuelle Zustand einer Maschine oder Komponente beschrieben werden kann. Diese Informationen in Kombination mit dem Arbeitsfortschritt bieten dem Betreiber Transparenz- und damit Effizienzsteigerungspotential. Neben den in der Instanz-Verwaltungsschale abgelegten Informationen, die für Konstruktion, Produktionsplanung, Instandhaltung etc. erforderlich sind, bietet auch eine Digitalisierung der Maschinensicherheit weiteres Effizienz- und Produktivitätssteigerungspotential. Nachdem in den Whitepaper 2018 „Safety in modularen Industrie 4.0-Produktionsanlagen“ [2] und 2019 „Smart Safety – Safety in Modular Production Processes“ [3] ein mögliches Konzept mit Entscheidungsbäumen und Safety-Agent vorgestellt wurde, stellt sich die Frage nach den weiteren erforderlichen Schritten in Richtung Umsetzbarkeit.

4. Plug&Produce: Anforderungen an die digitale Repräsentanz

In der digitalen Repräsentanz, bspw. Verwaltungsschale, einer Maschine oder eines Anlagenteils müssen die Informationen abgelegt werden, die später für die verschiedenen thematischen Fragestellungen oder Abteilungen der Organisation relevant sind. Eine Aufbereitung bzw. Verlinkung auf die Informationen in einer kontextuellen Betrachtungsweise einer Maschine wäre wünschenswert. Aus diesem Grund wird bspw. im Rahmen der Unterlage „Verwaltungsschale in der Praxis" [4] der Plattform I4.0 auf verschiedene Betrachtungsweisen verwiesen, bspw. Datenblatt, Dokumentation, Umgebung oder Equipment Information.

Zusätzlich zu den v. g. Überlegungen könnte für einen Betreiber eine Aufbereitung, der mit einer Maschine im Zusammenhang stehenden und digital abgelegten Informationen, entsprechend der nachfolgenden vorgeschlagenen Betrachtungsweisen hilfreich sein:

- organisatorische
- fachliche oder
- ereignisabhängige Betrachtungsweisen

Die organisatorischen Betrachtungsweisen würden die Inhalte des digitalen Zwillings oder der Verwaltungsschale anzeigen, die für die einzelnen Abteilungen, wie Einkauf, Konstruktion, Produktion, Instandhaltung, Facility, Vertrieb, Logistik etc. von Interesse sind. Für einen Instandhalter sind bspw. die Schaltpläne oder das Handbuch interessant, während ein Einkäufer für die zu bestellenden Ersatzteile die Stückliste benötigt. Für die Produktionsverantwortlichen oder Vertrieb sind dagegen nicht nur statische, sondern eher dynamische Daten, wie der Produktionsfortschritt, von Interesse.

Fachliche Betrachtungsweisen könnten bspw. in Anlehnung an die Ausführungen des IIC zu „Trustworthiness", folgendermaßen eingeteilt werden:

- Sicherheit
  - Safety
  - Security
  - Datenschutz

- Betrieb
  - Zuverlässigkeit
  - Resilienz
  - Instandhaltungsaufwand

Betrachtet man die Enden der Entscheidungsbäume und die Aufgabenstellung eines Risk Reduction Agent aus dem Whitepaper 2019 „Smart Safety – Safety in Modular Production Processes" [3] wird ersichtlich, dass die Gefährdungen digital abgebildet und entsprechend verfügbar sein müssen, so dass diese Gefährdung (bzw. das resultierende Risiko) mit verfügbaren Schutzmaßnahmen, bspw. Schleuse vom benachbarten Maschinenmodul, gegenübergestellt werden können. Da in der digitalen Maschinenrepräsentanz, bspw. VWS, neben Safety relevanten Detailinformationen auch das Vorhandensein von Informationen zu anderen Bereichen erforderlich sein könnte, erscheint eine ereignisabhängige Betrachtungsweise als sinnhaft.

Die ereignisabhängigen Betrachtungsweisen könnten ebenfalls in Anlehnung an das „Trustworthiness"-Model des IIC untergliedert werden:

- Gefährdungen im Zusammenhang mit Safety, bspw. gemäß ISO 12100
- Cyber-Attacken
- Beeinträchtigung der Maschine durch Umgebung
- Menschliches Fehlverhalten
- Technische Störung

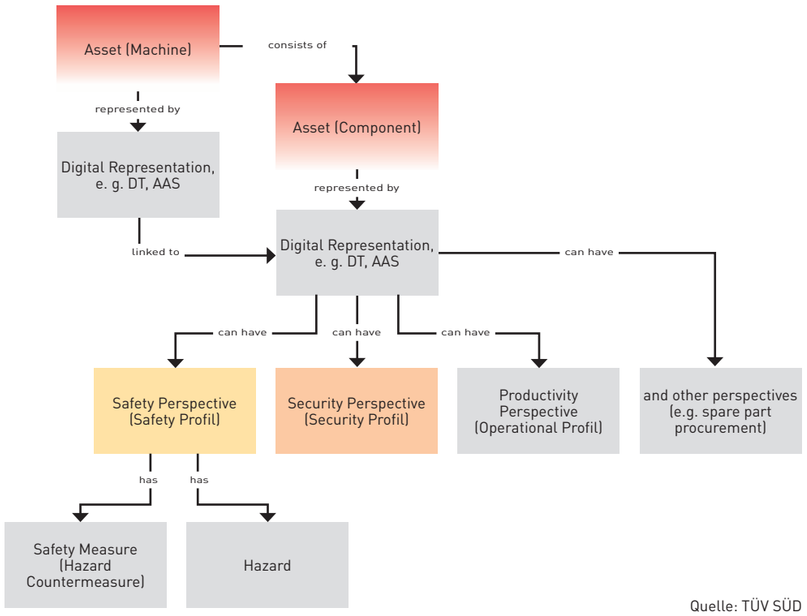
Festzustellen ist, dass die v. g. Überlegungen nicht nur für Plug&Produce gültig, sondern auf andere innovative Maschinensicherheits-Überlegungen übertragbar sind, wie nachfolgendes **Beispiel zur dynamischen Maschinensicherheit** zeigt:

Bei einer Plasmaschneideanlage können bei der Bearbeitung von bestimmten Materialien giftige Dämpfe entstehen. Der Ausfall der Absauganlage würde dazu führen, dass der Prozess abgebrochen wird und das Werkstück letztendlich Ausschuss wäre. Dies bedeutet für den Betreiber der Maschine Geldverlust in Form von Arbeitszeit und Material.

Mit der Kenntnis, dass kein Mensch anwesend ist und der Schneidprozess kurz vor Abschluss steht, kann in diesem Gedankenexperiment davon ausgegangen werden, dass bei einer Störung der Absauganlage in Kombination mit der Aufforderung „Raum lüften" sich keine unzulässige Menge an giftigen Dämpfen ansammelt. Eine dynamisierte Gestaltung der Maschinensicherheit könnte somit helfen die Produktivität zu steigern. Die konventionelle funktionale Sicherheit wäre weiterhin aktiv und würde, bei Nichtvorliegen von Umgebungsinformationen bei einer solchen technischen Störung sicherheitsgerichtet die Maschine abschalten.

Im Zusammenhang mit den verschiedenen Begriffen und oben eingeführten Betrachtungsweisen ist eine eindeutige Verwendung unabdingbar. Die „Betrachtungsweise Gefährdung" eines Assets würde die mit diesem Asset verbundenen spezifischen Einzel-Gefährdungen oder Instanz-Gefährdungen auflisten. Während im Rahmen einer Maschinensicherheitsbewertung, vgl. Whitepaper 2019 „Smart Safety – Safety in Modular Production Processes" [3], mit Hilfe von einem „Risk Reduction Agent" die einzelne Gefährdung bzw. Risiko mit einer Schutzmaßnahme gegenübergestellt und bewertet wird.

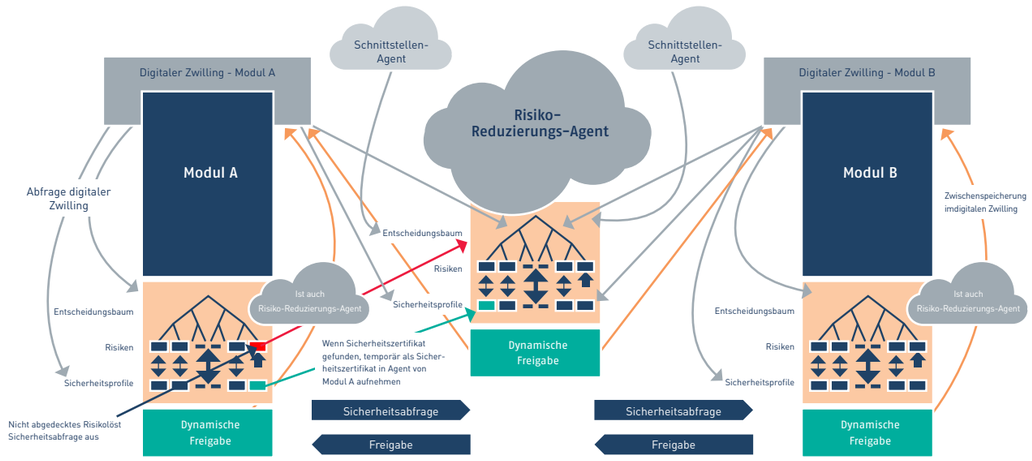
Für das Asset einer Maschine, bestehend aus verschiedenen Komponenten, ergibt sich somit bei Betrachtung der digitalen Maschinenrepräsentanz unter Berücksichtigung der fachlichen Betrachtungsweise sowie (Instanz-)Schutzmaßnahmen und (Instanz-)Gefährdungen folgendes Beziehungsdiagramm:



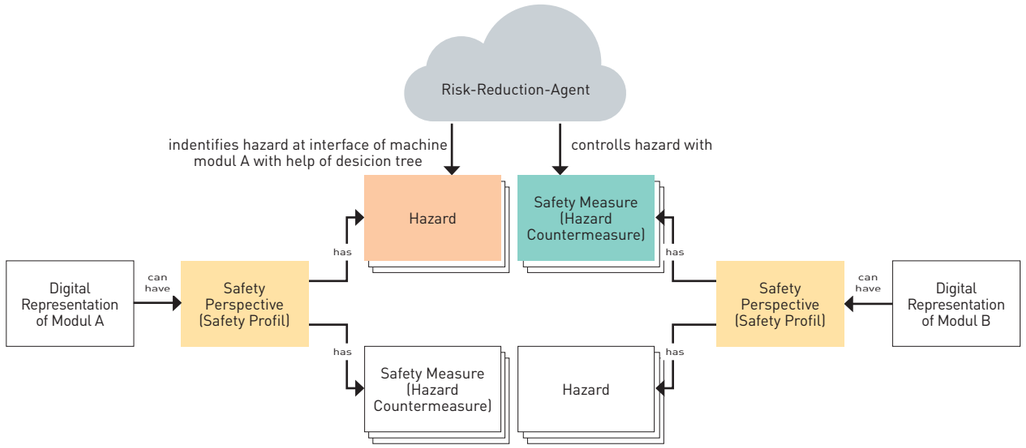
Quelle: TÜV SÜD

Dieser modulare Aufbau ermöglicht das einfache digitale Austauschen einer Komponente einer Maschine und damit automatisch eine Aktualisierung der mit der Maschine verbundenen Gefährdungen oder Schutzmaßnahmen. Diese Möglichkeit ist wichtig, da sich mit dem Austausch einer Komponente gegen eine nicht-typgleiche Komponente die Gefährdungssituation einer Maschine ändern kann. Wird beispielsweise bei einer Drehmaschine die Spindel mit Spindelantrieb gegen ein leistungsfähigeres Modell getauscht, ergibt sich durch eine höhere maximale Drehzahl eine andere Gefährdungssituation hinsichtlich des potenziellen Wegschleuderns von Teilen.

Nachfolgende Abbildung zeigt, wie sich die mit diesem Whitepaper eingeführte Struktur in das aus dem Whitepaper 2019 „Smart Safety – Safety in Modular Production Processes" [3] bekannte Konzept einfügt:



Damit der, mit dem Whitepaper 2019 „Smart Safety – Safety in Modular Production Processes“ [3], eingeführte „Risk Reduction Agent“ seine Aufgabe, der Überwachung der Maschinensicherheit nachkommen kann, sind jedoch Anforderungen an die Art und Weise der digitalen Repräsentanz einer Schutzmaßnahme oder einer Gefährdung zu definieren und zu standardisieren.



Mit den nachfolgenden Ausführungen wird ersichtlich, dass eine ausschließliche Gegenüberstellung einer Gefährdung (bzw. des resultierenden Risikos) mit einer Schutzmaßnahme den Ansprüchen nach einer möglichst unterbrechungsfreien Produktion nicht gerecht wird. Ein „Risk Reduction Agent“ ist in seiner Funktionalität somit nicht ausreichend. Aus diesem Grund wird im Weiteren von funktionserweiterten Agenten, nämlich „Smart-Safety-Agenten“ gesprochen.

Als Teil des Safety-Profils (oder Safety-Teilmodell) könnte die digitale Beschreibung einer Schutzmaßnahme daher die folgenden Aspekte, einschließlich wichtiger Links zu anderen Profilen oder Teilmodellen wie beispielsweise "Betrieb", enthalten:

(Die nachfolgende exemplarische Auflistung dient als Denkanstoß zur Diskussion und zukünftiger Weiterentwicklung; es wird keinen Anspruch auf Vollständigkeit erhoben.)

- Art der Komponente, z.B. Not-Aus-Taster, Schleuse
- Zustand, z.B. offen, geschlossen etc.
- Klassifizierung von Sicherheitsmaßnahmen, z.B. Kollisionsvermeidung, Abdecken etc.
- Eigenschaften der Sicherheitsmaßnahme, z.B. „Maschenweite“ einer trennenden Schutzeinrichtung oder Bremsweg etc.
- Räumliche Koordinaten der Schutzmaßnahme oder Safety-Komponente, z. B. in Bezug auf die Maschine
- Räumliche Manifestation, z. B. Größe der Toröffnung
- Anforderungen an die Verfügbarkeit, z. B. Verfügbarkeit der Hydraulik oder Pneumatik
- Zuverlässigkeit (Performance Level oder Reliability Level für mechanische Teile)
- Anforderungen an die Cybersecurity:
- Vertraulichkeit, Integrität und Verfügbarkeit
- Funktion der Schwere des Schadens
- Operativer Index (Auswirkung der Schutzmaßnahme auf Prozessablauf/Produktivität)
- Instandhaltungsindex (Auswirkung der Schutzmaßnahme auf die Instandhaltung)

Während die meisten Parameter für Safety-vertraute Personen selbsterklärend sind, erscheinen Aspekte wie „Operativer Index“ oder „Instandhaltungsindex“ als erklärungsbedürftig. Sind in einem Beispiel zwei Schutzmaßnahmen verfügbar, die im konkreten Anwendungsbeispiel als gleichwertig einzustufen sind, aber nur eine benötigt wird, sollte die Auswahl nicht zufällig erfolgen, sondern es sollte die Schutzmaßnahme der beiden herangezogen werden, welche den geringeren negativen Einfluss auf die Produktivität hat und den geringeren Instandhaltungsaufwand erfordert. Hierzu kann als Beispiel die Gegenüberstellung einer Schleuse mit einem Lichtvorhang aufgeführt werden. In der Regel hat ein Lichtvorhang einen geringeren Einfluss auf den zeitlichen Produktionsablauf als eine Schleuse, da mit dem Öffnen und Schließen ein höherer zeitlicher Aufwand verbunden ist, als eine entsprechende Schaltung des Lichtvorhangs.

Analog zu den Schutzmaßnahmen, muss eine digitale Repräsentanz für Gefährdungen vorhanden sein, die die einzelne Gefährdung bspw. hinsichtlich Art, Ort, Wirkrichtung, räumlicher und zeitlicher Ausprägung, Betrag (bspw. Energiegehalt [J]) etc. beschreibt. Es ist jedoch nicht ausreichend, die Gefährdungen, wie

Anmerkung: Wie in diesem Beispiel das Sicherstellen eines bestimmten Abstandes in der Praxis aussehen könnte, ist nicht Gegenstand dieser Überlegungen, sondern die Fähigkeit eine Schutzmaßnahme mit einer Gefährdung zu vergleichen.

diese in der EN ISO 12100 genannt werden (bspw. Beschleunigung, rotierende Teile, Spannung) wiederzugeben; es ist erforderlich, dass sinnhafte Gefährdungs-Gruppierungen erarbeitet werden, so dass die Gefährdungen maschinenlesbar werden. Dem Smart-Safety-Agent wird dadurch ermöglicht, eine Schutzmaßnahme mit einer bestimmten Gefährdung (bzw. das resultierende Risiko) zu vergleichen. Das heißt, es ist eine Sprache (Safety-Semantik) erforderlich, die das Problem hinter einer Gefährdung beschreibt. Ohne eine standardisierte Safety-Semantik wäre der Smart-Safety-Agent nicht in der Lage, eine Übereinstimmung zwischen einer Gefährdung und einer geeigneten Schutzmaßnahme zu finden.

Zum Beispiel können die Gefahren, wie Beweglichkeit der Maschine oder Verbrennen von einem Schweißbrenner, mit einer trennenden Schutzeinrichtung (z.B. geschlossene Schleuse) oder mit Abstand zwischen der Gefahrenstelle und einem Menschen beherrscht werden. Beide Beispiele einer Schutzmaßnahme können das Problem lösen. Aus der Sicht der Fertigung kann es Vorteile haben, eine Schleuse offen zu lassen, um insgesamt schneller zu sein, und einen Sicherheitsabstand zu gewährleisten. Das bedeutet, dass der Smart-Safety-Agent in der Lage sein muss, zu verstehen, dass beide Schutzmaßnahmen auf die zu beherrschende Gefährdung anwendbar sind. Um diese Art von Vergleich mit einem Computer durchführen zu können, ist somit eine geeignete Gruppierung der Gefährdungen erforderlich. Eine Gefährdungsgruppierung könnte mit Hilfe des Problems hinter einer Gefährdung vorgenommen werden, z. B. im Falle von einer bewegten Maschine oder Flamme von einem Schweißbrenner muss sichergestellt werden, dass es während des Betriebs zu keiner Kollision bzw. Kontakt zwischen dem gefährlichen Teil der Maschine und einem Menschen kommt. Diese Gefährdungsgruppierung (= Teil der Safety Semantik) muss standardisiert werden, um Interoperabilität und sicheren Betrieb zu gewährleisten.

Als zusammenfassendes Beispiel ist ein AGV (= autonomous guided vehicle) zu nennen, das auf die Gefährdungen Zusammenstoß, Anstreifen etc. (Problem hinter den Gefährdungen: „Kontakt verhindern“) mit den Aktionen „stehen bleiben“, „Routenänderung“ oder „Fahrspuranfrage“ reagieren kann. Die Aktion „Fahrspuranfrage“ ist jedoch nur im Zusammenhang mit Maschinen (z. B. Hallentor) sinnig, wenn diese antworten können. In diesem Beispiel würde der Smart-Safety-Agent eine Routenänderung vorschlagen, bevor das AGV in einen aktuell von Menschen stark frequentierten Kreuzungsbereich einfährt und aufgrund der Kollisionsdetektionssensorik stehen bleibt. Dies bedeutet es würde die heute übliche Schutzmaßnahme „Stillstand“ durch die Schutzmaßnahme „Sicherheitsabstand“, implementiert durch Routenänderung, ersetzt werden. Die durch die funktionale Sicherheit abgesicherte Kollisionserkennung wäre weiterhin aktiv und als „fall back“-Lösung verfügbar.

Der Smart-Safety-Agent stellt somit eine Erweiterung zur heutigen funktionalen Sicherheit dar, d.h. es handelt sich bei dem Ansatz der Smart-Safety, wie dieser hier beschrieben ist, um ein mehrstufiges Konzept, das in der untersten Stufe, hier als „fall back“-Lösung bezeichnet, ausschließlich die bekannte funktionale Sicherheit beinhaltet und davon unabhängige erweiternde Funktionen in den höheren Stufen zur Verfügung stellt. Dieses Setup ermöglicht die Effizienz in der Nutzung von Maschinen und Anlagen und damit die Produktivität weiter zu steigern.

5. Safety-Informationsmodel

Der oben hergeleitete Aufbau begründet sich in der Verarbeitbarkeit von Safety-relevanten Eigenschaften und Parametern bspw. bei Umbauten einer Anlage oder eines Maschinenmoduls, da dies als Erfordernis eines generischen Informationsmodelles gesehen wird. Im Folgenden in Kurzform dargestellt:

Die Daten-Grundlage für das **Safety-Teilmodell** der Verwaltungssschale sollte ein Informationsmodell mit Inhalt, wie oben hergeleitet, der Schutzmaßnahmen und der Gefährdungen sein. Das Informationsmodell für die Gefährdungen (innere und äußere, bspw. mech. Gefährdungen, el. Gefährdungen etc. vgl. DIN EN ISO 12100) würde vergleichbar wie das Informationsmodell der Schutzmaßnahmen aussehen.

Es stellt sich die Frage, nachdem Anforderungen an den Inhalt gestellt wurden, wie ein **Safety Layer** aussehen könnte?

Ein Safety Layer muss eindeutig einer Anlage, Maschine bzw. Komponente, also einem Asset, zugeordnet werden. Dies kann mit einem Submodul in der entsprechenden Verwaltungsschale realisiert werden. Das Submodel Safety Layer bezieht sich auf die eigene, einmalig vergebene, Referenz-Id und sollte mit einer „idShort = Safety_Layer" beschrieben werden. Die einzelnen Safety-relevanten Profile können mit „Properties" in dem Submodul Safety Layer integriert werden. Im Hinblick auf modulare Anlagen müssen diese Eigenschaften von der Kategorie „Variable" sein, da sich der Wert des Sicherheitsprofil während der Laufzeit überprüft und ggf. geändert wird. Im Umkehrschluss bedeutet es für die VWS des Moduls, dass dieses auch die Rechte zum Auslesen anderer Module bereitstellen muss. Durch entsprechende Verweise auf der Typ-Verwaltungsschale kann auf das Submodel referenziert werden. Für verteilte Kontrollsysteme bietet die IEC 61499 eine standardisierte Modellierungssprache und eine Architektur im Industrie 4.0 Kontext [5]. Neben Variablen kann das Teilmodell auch Methoden (Operationen) beinhalten, um Aktionen auszuführen, z.B. Fähigkeit zur Prüfung oder zur Risikoreduktion / -vermeidung.

Wie oben schon beschrieben, ist es für modulare Anlagen notwendig die sicherheitstechnischen Profile auszutauschen und sie zu verstehen, ob im kombinierten Zustand der Anlage alle sicherheitstechnischen Funktionen greifen und funktionieren. Der Austausch und das gemeinsame Verständnis der digitalen Repräsentanzen, sowie Anlagen, erfordert eine Semantik, wie z.B. eCl@ss. Über die standardisierten Merkmale und Stammdaten von Produktklassen lässt sich schon heute auf eine Vielzahl von Produkten und Dienstleistungen zugreifen. Des Weiteren findet man in der IEC 61360 und ISO 13584 Standarddatenelementtypen und die dazugehörigen Klassifizierungsschema, die für eine semantische Beschreibung der VWS dienen können.

Literatur:

[1] Platform Industrie 4.0: Part 1 – The exchange of information between partners in the value chain of Industrie 4.0 (Version 2.0), Federal Ministry for Economic Affairs and Energy (BMWi), 2019

[2] Technologie-Initiative ***SmartFactory***^{KL} e.V., Safety an modularen Maschinen; Whitepaper SF-3.1: 04/2018

[3] Technologie-Initiative ***SmartFactory***^{KL} e.V., Smart Safety – Sicherheit in modularen Produktionsprozessen; Whitepaper SF-3.2: 04/2019

[4] M. Wenger, T. Müller, Connecting PLCs with their Asset Administration Shell for Automatic Device Configuration, IEEE 16th International Conference on Industrial Informatics (INDIN), 2018

[5] Plattform Industrie 4.0: Diskussionspapier Verwaltungsschale in der Praxis https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/2019-verwaltungsschale-in-der-praxis.pdf?__blob=publicationFile&v=11

Versionshistorie
Whitepaper SF-3.3: 09/2020

Herausgegeben von
Technologie-Initiative SmartFactory KL e.V.
Trippstadter Straße 122
67663 Kaiserslautern

T +49 (0)631 20575-3401
F +49 (0)631 20575-3402

Die Technologie-Initiative SmartFactory KL e.V. (*SmartFactory*^{KL}) ist ein gemeinnütziger Verein des öffentlichen Rechts, eingetragen im Vereinsregister Kaiserslautern.

Vereinsregisternummer: VR 2458 Kai

Vorstand
Prof. Dr. Martin Ruskowski (Vorsitzender)
Andreas Huhmann, HARTING AG & Co. KG
Klaus Stark, Pilz GmbH & Co. KG
Dr. Haike Frank, SCHOTT AG

Wissenschaftlicher Koordinator
Dr.-Ing. Achim Wagner
T +49 (0)631 20575-5237
M achim.wagner@smartfactory.de