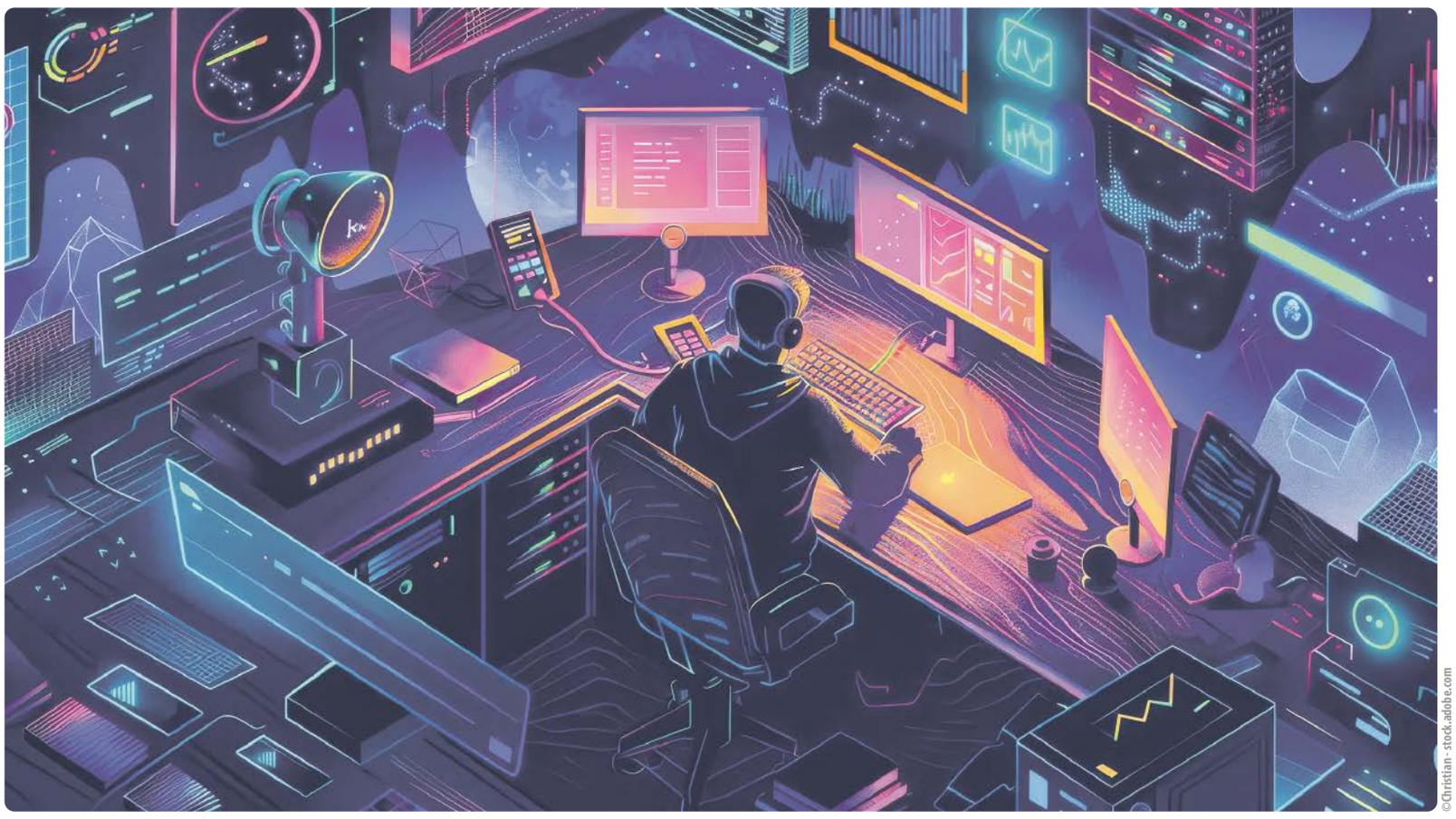
# Security Management

## NE 193: Ein Informationsmodell für das Automation Security Engineering



©Christian - stock.adobe.com

Die NAMUR-Empfehlung NE 193 definiert ein Informationsmodell für das Security Engineering von Automatisierungssystemen (Automation Security Engineering), also das Analysieren von Security-Problemen, das Treffen von Security-Entscheidungen und das Entwickeln von Security-Lösungen für Automatisierungssysteme.

© ralfbaumgarten

> *Mit dem in der NE 193 beschriebenen Informationsmodell kann die OT-Security besser diskutiert und dokumentiert werden.*
>
> Andreas Schüller, Yncoris

Das vom NAMUR-Arbeitskreis 1.3 „Informationsmanagement und Werkzeuge“ unter der Leitung von Andreas Schüller, Yncoris, erarbeitete Dokument beschreibt ein UML-Informationsmodell (Unified Modeling Language ist eine visuelle Modellierungssprache für die Architektur, das Design und die Implementierung von komplexen Softwaresystemen und besteht aus verschiedenen Diagrammarten), das die für das Automation Security Engineering notwendigen und während des Security Engineering entstehenden Informationen beinhaltet. Es ist für das Automation Security Engineering in der Design- und Betriebsphase eines Automatisierungssystems nutzbar und kann von Herstellern, Integratoren und Betreibern gleichermaßen verwendet werden – branchen- und standortunabhängig.

Der Anwendungsbereich des Informationsmodells ist die Dokumentation der Informationen, die beim Security-Engineering eines Automatisierungssystems verwendet und/oder erzeugt werden. Es dokumentiert also die Security von Automatisierungssystemen. Die Security der Informationen im Informationsmodell wird in dieser NAMUR-Empfehlung nicht betrachtet.

### Zielsetzung

„Heutzutage wird die OT-Security meist nachgelagert zum Engineering des Automatisierungssystems betrachtet. Durch das in der NE 193 beschriebene Informationsmodell kann die OT-Security früher und verzahnter mit anderen Gewerken im Planungsprozess diskutiert und direkt im Modell dokumentiert werden. Die NE 193 ermöglicht ein Security by Design von Automatisierungssystemen in der Prozessindustrie“ erläutert Andreas Schüller gegenüber CHEManager. Und Sarah Fluchs von Admeritia, die maßgeblich an der Erstellung des Dokuments beteiligt war, betont: „Das Security Engineering für Automatisierungssysteme ist eine ziemlich junge Disziplin; es ist noch nicht so klar wie in anderen Domänen, was genau eigentlich „Automation Security-Daten“ sind. Mit der NE 193 haben wir dafür einen ersten Wurf gemacht – und zwar gleich so, dass die Daten auch digital verarbeitet werden können, also in einem formalen UML-Informationsmodell.“

### Anwendungsfälle

„Verwaltungsschale, digitaler Zwilling, Industrie 4.0: Alle Ingenieurdomänen sind gerade dabei, ihre über Jahrzehnte analog angesammelten Daten digital verfügbar zu machen. Damit das klappt, braucht man Informationsmodelle“ ordnet Fluchs das Dokument ein, das für das Automation Security Engineering verschiedene Anwendungsfälle hat:

- **Informationsaustausch zwischen Security-relevanten Planungswerkzeugen:** Security-relevante Informationen gibt es in vielen verschiedenen Softwarewerkzeugen bzw. Dateien: in IT Administrationstools wie Asset-Inventaren, Konfigurationsmanagement- oder Versionierungstools, in dedizierten Security Tools wie Anomalieerkennungs- oder Intrusion-Detection-Systemen, aber auch in Engineering-Werkzeugen, die Risikobetrachtungen oder architekturelle Entscheidungen enthalten. Es ist unwahrscheinlich, dass diese verschiedenen Werkzeuge ihre Datenformate in absehbarer Zeit harmonisieren werden, weshalb ein neutrales Informationsmodell zum Austausch der Security-relevanten Informationen die pragmatischere Lösung zu sein scheint.

© LTsoft

> *Eine zunehmende externe Bedrohungslage macht ein systematisches Management der Security unumgänglich.*
>
> Björn Höper, LTsoft

- **Modellbasiertes Security Engineering und Security by Design:** Ein Informationsmodell ist die Basis, um modellbasiertes Security Engineering zu ermöglichen und flexible Visualisierungen des zu schützenden Systems, seiner Security-Probleme bzw. der Security-Lösungen zu erzeugen. Ein Informationsmodell für das Security Engineering hilft auch dabei, Security möglichst früh in den Automation-Engineering-Workflow zu integrieren (Security by Design) – so kann man schon Security-Entscheidungen treffen, auch wenn das Detail Engineering noch nicht abgeschlossen ist.

- **Treffen von Security-Entscheidungen während des Betriebs:** Security-Entscheidungen wie das Patchen einer Schwachstelle oder das Anwenden einer Alternativmaßnahme für Schwachstellen, für die kein Patch verfügbar ist, erfordern Kontextinformationen aus typischerweise verschiedenen Quellen. Relevant sind z.B. der Schweregrad der Schwachstelle, die bestehenden Risiken und frühere Vorfälle für eine Komponente, die Kritikalität des Versagens oder der Manipulation der Komponente, die Netzwerkexposition der Komponente und die Kritikalität der daran angeschlossenen Komponenten. Diese Informationen sind jedoch wahrscheinlich an verschiedenen Orten gespeichert und müssten zeitaufwändig gesammelt und verarbeitet werden – sofern sie überhaupt verfügbar sind. Ein Informationsmodell hilft, alle Security-relevanten Engineering-Informationen auch in der Betriebsphase noch verfügbar zu haben.

© admeritia

> *Der Austausch von Informationen zwischen Herstellern und Betreibern wird wichtig vor dem Hintergrund des Cyber Resilience Act.*
>
> Sarah Fluchs, Admeritia

- **Verwaltung von Standardkonfigurationen:** Effizienzgewinne im Betrieb von Security-Lösungen ergeben sich oft aus der Standardisierung von Komponenten und ihren Konfigurationen. Diese Standards müssen maschinenverarbeitbar gespeichert, gepflegt und verwaltet werden. Selten deckt ein Tool alle relevanten Informationen ab. Solche Standardkonfigurationen über viele Tools verteilt zu speichern und zu pflegen ist jedoch fehleranfällig und ineffizient.

### Ausblick

Für all diese Anwendungsfälle besteht der Wert des Informationsmodells in der Einigung auf ein generisches Modell, das alle Beteiligten nutzen. Das Ziel der NAMUR-Empfehlung ist, einen Vorschlag für solch ein konsensfähiges Modell zu machen. Fluchs dazu: „Wir hoffen auf breite Nutzung und viele Verbesserungsvorschläge aus der Praxis, denn ein Informationsmodell ist nur dann etwas wert, wenn es viele nutzen. Damit wäre es zum Beispiel möglich, relevante Informationen für das Automation Security Engineering zwischen Herstellern und Betreibern auszutauschen – das wird wichtig vor dem Hintergrund des Cyber Resilience Act, oder zwischen verschiedenen Security-Tools, die ein Betreiber im Einsatz hat – zum Beispiel Asset Inventory-, Intrusion Detection- und Risikoanalyse-Tools.“ Und Björn Höper von LTsoft, ebenfalls Mitglied des AK 1.3, fasst die Notwendigkeit zur Umsetzung eines systematischen Managements der Security in der Prozessindustrie zusammen: „Als IT/OT-Systemintegrator erleben wir eine deutliche Beschleunigung der notwendigen Anpassungen an den Landscapes unserer Kunden und eine ebenso deutliche Zunahme der Komplexität. Die Verbindung dieser Faktoren mit steigenden regulatorischen Anforderungen wie bspw. NIS2 und einer zunehmenden externen Bedrohungslage machen ein systematisches Management der Security unumgänglich, um die Intellectual Property und die Betriebsfähigkeit der Unternehmen zu schützen. Mit dem Security-Informationsmodell haben wir ein Werkzeug geschaffen, mit dem diese Aufgabe formalisiert und effizient erledigt werden kann.“

*Volker Oestreich, CHEManager*

■ www.namur.de

**KOLUMNE: PROZESSINDUSTRIE**

## Die Macht datengetriebener Zusammenarbeit

**Christine Oro Saavedra, NAMUR**

© Bayer

**Christian Bünger, Verband der Chemischen Industrie (VCI)**

© VCI

Die Prozessindustrie wandelt sich sukzessive vom Materiallieferanten zum Lösungs- und Serviceanbieter. Ein zentraler Baustein dieser Entwicklung sind branchenübergreifende Datenräume, um Daten sicher und effizient auch über Firmen- und Sektorengrenzen hinweg zu teilen und für entsprechende Anwendungsfälle (z.B. Data-Mining, Prozessoptimierung, Supply Chain) zu nutzen. Doch was genau bedeutet das für die Prozessindustrie und insbesondere für die chemische Produktion? Datenräume sind kollaborative Plattformen, die es Unternehmen ermöglichen, Dritten Daten unter definierten Bedingungen zur Verfügung zu stellen. In der chemischen Produktion spielen diese eine wichtige Rolle, da sie die Grundlage für datengetriebene (Geschäfts-) Prozesse bilden. Sie ermöglichen eine verbesserte Entscheidungsfindung, die Optimierung von Produktionsprozessen und die Entwicklung neuer Geschäftsmodelle. Ein konkretes Beispiel hierfür ist die Initiative Catena-X, die als erster offener und kollaborativer Datenraum für die Automobilindustrie dient und als Vorbild für die Prozessindustrie, einschließlich der chemischen Produktion, betrachtet werden kann!

### Effektiver Informationsaustausch in der Prozessindustrie

Eine digitale Plattform, die den Kern für den Datenraum darstellt, bietet die Möglichkeiten, Daten sicher (Cybersecurity) und compliant auszutauschen bzw. zu übermitteln. Die Spielregeln (Governance) in diesem Datenraum sind eindeutig definiert und ermöglichen schnelle und effiziente Vertragsabschlüsse. Datenräume sind ein Baustein der digitalen Infrastruktur und werden aktuell von vielen verschiedenen Branchen errichtet. Als Vorreiter ist hier die Automobilindustrie zu sehen. Wir als Prozessindustrie und Chemieindustrie wollen diese Entwicklung aktiv mitgestalten, damit zukünftige Datenräume optimal zu unseren spezifischen Anforderungen passen. Kombiniert mit anderen bereits existierenden Standards wie der Asset Administration Shell (AAS), NAMUR Open Architecture (NOA) und Module Type Package (MTP) helfen sie uns, die bevorstehenden Aufgaben anzugehen und langfristig zu verwalten.

Die chemische Produktion steht bereits jetzt vor einer Reihe von Herausforderungen, die es zu meistern gilt. Eine dieser Herausforderungen ist die sichere Marktversorgung mit wichtigen alltäglichen Produkten. Engpässe bei der Produktion können unter Umständen schwerwiegende Folgen haben. Dies hat uns die Coronapandemie schmerzhaft vor Augen geführt.

Datenräume bieten vielversprechende Lösungsansätze für Themen, die uns aktuell bewegen. Durch transparentere Bedarfsprognosen lässt sich die Produktion besser planen und Engpässe können vermieden werden. Eine optimale Planung führt zu einer stabileren Marktversorgung. Die Berechnung der verbleibenden Nutzungsdauer (Remaining Useful Lifetime) von technischem Equipment und die vorausschauende Instandhaltung (Predictive Maintenance) der Geräte ermöglichen es, Fachpersonal gezielt dort einzusetzen, wo tatsächlich Bedarf an Instandhaltung oder Kalibrierung besteht und Geräte nur dann auszutauschen, wenn sie tatsächlich nicht mehr zuverlässig betrieben werden können. Vorausschauende Planung spart damit auch Kosten, denn ungeplante Downtime wird somit vermieden. Durch die Kombination von Daten aus dem Gerät selbst über das NOA-Informationsmodell und statistische Auswertungen aus Fehlerdatenbanken wie NAMUR.Smart werden solche Ansätze möglich.

### Prozessindustrie zukunftssicher gestalten

Für die erfolgreiche Implementierung von Datenräumen sind allerdings etliche Voraussetzungen zu erfüllen. Für einige Anwendungen müssen zunächst die Teilmodelle der sog. Verwaltungsschalen erstellt werden. In den Firmen müssen entsprechende Ablagesysteme für die Daten aufgebaut werden. Auch müssen Routing-Komponenten und diverse Adapter (z.B. für ERP-Systeme und andere Datenbanken) entwickelt werden. Die Rahmenbedingungen, insbesondere zum Marktplatzdesign, zur Sicherheit und zum Zugriffsmanagement, werden derzeit im Rahmen aller Manufacturing-X-Projekte ausgehandelt und ausgearbeitet. Diese können einfach kopiert und für den individuellen Bedarf adaptiert werden.

Datenräume bieten eine immense Chance, die Prozessindustrie zukunftssicher zu gestalten. Sie ermöglichen es, die aktuellen Herausforderungen langfristig zu meistern und gleichzeitig neue Geschäftsbereiche zu erschließen. Wir, NAMUR und VCI, laden alle Interessierten ein, sich an dieser zukunftsweisenden Entwicklung zu beteiligen. Gemeinsam können wir die Zukunft der Prozessindustrie gestalten und sicherstellen, dass sie den Anforderungen von morgen gerecht wird. Mitgestalter sind herzlich willkommen!

■ office@namur.de
■ www.namur.de

**Emerson ist Sponsor der NAMUR-Hauptsitzung 2024**