atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 10 2022

Gemeinsame Nutzung der PLT: Betriebs- und Sicherheitseinrichtungen richtig absichern

Felix Kahrau, Erwin Kruschitz, Jan Russmann, Benedikt Bittcher, Detlef Winkel

Das Risiko, dass auch Sicherheitseinrichtungen durch Cyberbedrohungen manipuliert werden, steigt erheblich. Die Einschätzung solcher Risiken ist insbesondere dann komplex, wenn Komponenten sowohl für Sicherheitsfunktionen als auch für betriebliche Funktionen genutzt werden.Ein Experten-Team verschiedener Chemiekonzerne erklärt in diesem Beitrag nicht nur, wie sich das Cyberrisiko durch gemeinsame Nutzung verändert, sondern auch wie es evaluiert und mit welchen Maßnahmen eingedämmt werden kann.

1. Einleitung

PLT-Betriebseinrichtungen dienen der Steuerung von verfahrenstechnischen Prozessen. PLT-Sicherheitseinrichtungen (nach IEC 61511) dienen dem Schutz vor Schäden für Gesundheit und Umwelt. In der automatisierungstechnischen Praxis ist die gemeinsame Nutzung verschiedenster Komponenten durch Betriebs- und Sicherheitseinrichtungen durchaus üblich. Solche „gemeinsam genutzten Komponenten“ sind auf allen Ebenen der Automatisierungspyramide zu finden: Sensoren, Aktoren, Steuerungen (*Logic-Solver*), Programmierstationen (*Engineering Station*, *Asset Management*), Netzwerkkomponenten und IT-Dienste wie z. B. Benutzerauthentifizierung, Patchen, Virenscanner, Backup, Datenhaltung.

Nach den gültigen technischen Regeln sollten PLT-Sicherheitseinrichtungen und PLT-Betriebseinrichtungen möglichst voneinander getrennt und unabhängig (separiert) sein, um Ausfälle gemeinsamer Ursache und -in weiterer Folge- ein unerwünschtes Ereignis zu vermeiden.

Neuerdings ist auch das Auftreten von Cyberbedrohungen bei der Beurteilung der Praxis der gemeinsamen Nutzung zu berücksichtigen. Die Frage „Ist meine Anlage auch angesichts von Cyberbedrohungen sicher?“ muss klar beantwortet werden können.

Vor diesem Hintergrund hat sich eine Expertengruppe aus verschiedenen Chemiekonzernen zusammengesetzt. Das Ziel war, die Frage nach der Sicherheit bei gemeinsamer Nutzung möglichst pauschal zu beantworten. Unter Zuhilfenahme einer speziellen Risikoanalysemethode wurde ermittelt, ob und in welcher Höhe, ein „Mehrrisiko“ durch gemeinsame Nutzung entsteht und wie dieses Risiko zu begründen ist. Untersucht wurden die Komponenten *Engineering-Station*, *Logic-Solver* und *OT-Infrastruktur*. Um ein möglichst allgemeingültiges Ergebnis zu erreichen, wurden die prinzipiellen Systemarchitekturen dreier Hersteller, eingebettet in drei verschiedene Konzernumgebungen (Regelwerke, Organisationsstrukturen und -kulturen) als Betrachtungsgrundlage herangezogen.

2. Was bedeutet „gemeinsame Nutzung“?

Abbildung 1 skizziert die idealisierte Vorstellung von Trennung, Unabhängigkeit und Diversität (die separate Nutzung) von Komponenten zur Umsetzung der PLT-Sicherheitsfunktion (rot) und der der PLT-Betriebsfunktion (blau).

Traditionell wird unter gemeinsamer Nutzung –im Gegensatz zu separater Nutzung-beispielsweise ein gemeinsam genutztes Ventil oder ein gemeinsam genutzter Logic-Solver verstanden. Aus Sicht der Cybersecurity ist es jedoch sinnvoll, den Begriff der gemeinsamen Nutzung zu erweitern. Dies ist notwendig, damit auch die cyber-relevanten Komponenten aus Zone B (nach NAMUR NA 163) und die verbundenen Funktionen aus der IT/OT-Infrastruktur in die Betrachtung aufgenommen werden können (s. Abbildung 2).

Dementsprechend wird von gemeinsamer Nutzung in diesem Beitrag dann ausgegangen, wenn die Kompromittierung eines einzelnen Assets Auswirkungen auf sowohl

» die PLT-Sicherheitsfunktion *als auch*

» die PLT-Betriebsfunktion

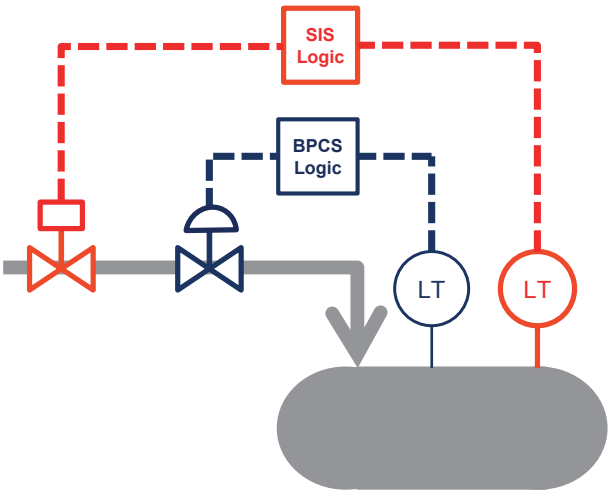

Abbildung 1: Separate Nutzung.

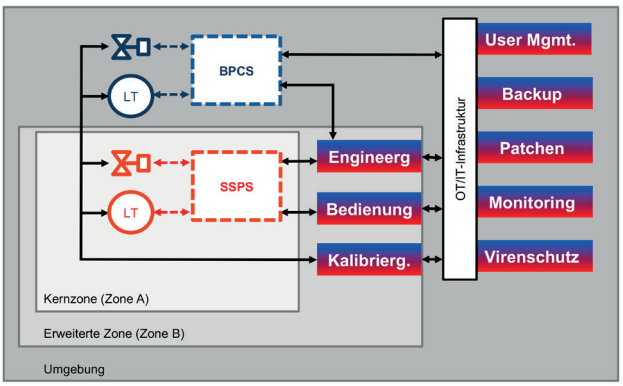

Abbildung 2: gemeinsame Nutzung in Zone B und Umgebung (rot/blau).

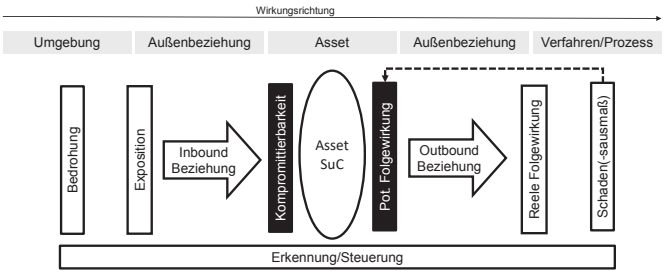

Abbildung 3: Wirkungsmodell der OT-Risiko-Komponenten.

haben kann. Generell kann unter dem Begriff „Asset“ eine Hard- oder Soft- oder Firmware, ein Dienst, ein Prozess oder auch eine Organisation verstanden werden.

3. Das Risiko gemeinsamer Nutzung und Cyberbedrohungen

Sowohl die Cybersecurity als auch die funktionale Sicherheit arbeitet mit dem Begriff „Risiko“. Beide Welten kennen verschiedene Verfahren zur Ermittlung des Risikos. Ein Begriffsabgleich war bis dato noch nicht erfolgreich. Entsprechend schwierig ist die Verständigung und Vergleichbarkeit. Um diese Defizite zu kompensieren und um Missverständnisse zu vermeiden, kann das in Abbildung 3 gezeigte Wirkungsmodell herangezogen werden. Es ersetzt den missverständlichen Risikobegriff durch eine diversifizierte Betrachtung von klar definierbaren Parametern. Im Zentrum der Betrachtung steht das Asset bzw. das zu betrachtende System (SuC), welches eine mehr oder weniger hohe Kompromittierbarkeit aufweist. Der Grad an Kompromittierbarkeit wird u. a. durch die Komplexität des Assets, durch Software-Schwachstellen oder fehlende Security-Maßnahmen beeinflusst.

Die Bedrohung besteht aus Art und Umfang (Wahrscheinlichkeit) mit der die Grundwerte (Integrität und Verfügbarkeit) des Assets durch eine exponierte Kompromittierbarkeit verletzt werden könnten.

Der negative Effekt eines kompromittierten Assets hängt zunächst davon ab, ob das Asset potenziell in der Lage ist, ein unerwünschtes Ereignis auszulösen, die PLT-Sicherheitsfunktion zur Vermeidung eines solchen Ereignisses zu unterdrücken oder – im ungünstigsten Fall – beides (potenzielle Folgewirkung).

Die Intensität der Außenbeziehung bestimmt, wie stark sich eine potenzielle Folgewirkung zu einer realen Folgewirkung entwickelt, die dann abhängig vom Prozessrisiko zu einem Schadensausmaß führt.

Ein weiterer Bewertungsaspekt ist die Möglichkeit eine Bedrohung, eine Kompromittierung oder eine Folgewirkung zu detektieren (Erkennung) und zu beeinflussen (Steuerung) z. B. automatisch entsprechende Gegenmaßnahmen einzuleiten.

4. Worin besteht das erhöhte Risiko durch gemeinsame Nutzung?

Legen wir das eben geschilderte Wirkungsmodell zu Grunde, lässt sich das Cyberrisiko eines separierten Systems mit dem eines gemeinsam genutzten Systems gegenüberstellen.

Dabei werden zur Ermittlung der Kompromittierbarkeit beispielsweise der physische und logische Zugangs- und Zutrittsschutz sowie vorhandene Schutzmaßnahmen, der Kompetenzstatus, der mit dem System im Zusammenhang stehenden Personen, und die Komplexität des Systems bewertet. Die Bewertung im vorliegenden Fall erfolgte semiquantitativ, basierend auf den Erfahrungswerten der beteiligten Experten. Zum Beispiel: Drei Minuspunkte wenn keine Schutzmaßnahmen nachweisbar sind. Zwei Punkte werden abgezogen, wenn die Einhaltung der vom Hersteller vorgegebenen Maßnahmen dokumentiert wurde und ein Punkt, wenn über die Herstellermaßnahmen hinaus die Sicherheitsmaßnahmen der NA 163 Checkliste nachgewiesen werden können. Das in Abbildung 4 dargestellte Ergebnis entstammt der Betrachtung der Komponente *Engineering Station*.

Dieser Beurteilung nach liegt das Cyberrisiko einer separierten *SIS Engineering Station* deutlich unter dem Risiko einer *gemeinsam genutzten Station* (GeNuIS). Die Ergebnisunterschiede sind im Detail wie folgt begründet:

Die Kompromittierbarkeit einer separierten SIS Engineering Station ist geringer (d. h. besser) da sich der Zugriff darauf auf SIS-Spezialisten beschränkt, bei denen von einem erhöhten Schulungs- und Kompetenzstatus (hinsichtlich der funktionalen Sicherheit) ausgegangen werden kann. Die geringere Anzahl der Nutzerinnen und Nutzer begünstigt den Faktor „Außenbeziehung“ und damit die Exposition.

Ein weiterer relevanter Faktor liegt in der potenziellen Folgewirkung. Denn: Im Falle einer gemeinsam genutzten Engineering Station muss davon ausgegangen werden, dass –im ungünstigsten Fall- durch eine Kompromittierung (z. B. des Logik-Programms) ein unerwünschtes Ereignis herbeigeführt und gleichzeitig das Auslösen der PLT-Sicherheitseinrichtung unterdrückt werden kann. Bei getrennten Engineering Stationen wäre lediglich eine der beiden Folgewirkungen anzunehmen.

Die durchgeführten Gegenüberstellungen von gemeinsamer Nutzung von Logic Solver und OT-Infrastruktur (Switche, Firewalls, Netzwerkverbindungen) kommen im Endergebnis zur gleichen Aussage. Die detaillierte Begründung unterscheidet sich abhängig von der konkreten Systemarchitektur.

Im Vergleich der drei Komponententypen hat sich gezeigt, dass das Cyberrisiko von gemeinsam genutzter Engineering Station etwa gleich hoch ist, wie das Risiko eines gemeinsam genutzten Logic-Solvers. Die gemeinsam genutzte OT-Infrastruktur weist dagegen einen höheren Risikowert aus. Dieser ergibt sich durch eine erhöhte Kompromittierbarkeit bei gleichzeitig höherem Vernetzungsgrad.

5. Zusammenfassung und Schlussfolgerungen

Das Ergebnis der Untersuchung ist eindeutig: Eine gemeinsame Nutzung – ohne entsprechende Gegenmaßnahmen – erhöht das Risiko für ein unerwünschtes Ereignis. Die Ursachen können primär damit begründet werden, dass die gemeinsame Nutzung es in vielen Fällen ermöglicht, durch einen unbefugten „Cybereingriff“ sowohl ein auslösendes Ereignis herbeizuführen als auch die Sicherheitsfunktion zu unterdrücken.

Zusätzlich führt die gemeinsame Nutzung zu einer erhöhten Exposition der jeweiligen Komponente durch vergleichsweise intensivere Außenbeziehungen. Unter Außenbeziehungen sind die höhere Anzahl von Personen mit Zugriff auf eine gemeinsam genutzte Komponente wie z. B. der Engineering Station sowie der höhere Vernetzungsgrad zu verstehen.

Den Vorteilen der gemeinsamen Nutzung (wie z. B. ein geringerer Schulungsaufwand, einfachere Strukturen, weniger Komponenten) stehen Nachteile durch erhöhte Cyberrisiken und entsprechenden Mehraufwand für Security-Maßnahmen gegenüber. Inwiefern das Gewicht der Vorteile überwiegt, hängt von Rahmenbedingungen wie Verfügbarkeit von Personal, Größe und Gefährlichkeit der Anlage, Anlagenalter und Vernetzungsgrad ab. Diese Abwägung wird weiterhin anlagenspezifisch durchgeführt werden müssen.

6. Ausblick

Für die Zukunft kann davon ausgegangen werden, dass die Vorteile der gemeinsamen Nutzung durch intensivierte Digitalisierung (Cloud, IT/OT-Convergence) sogar noch gesteigert werden können. Angesichts dieser Annahme erscheint eine weitere Beschäftigung mit der Frage nach der Cyberresilienz von gemeinsamer Nutzung dringend notwendig und sinnvoll.

Auf Basis der in dieser Analyse geförderten Erkenntnisse kann der in diesem Artikel gewählte semi-quantitative Ansatz in Richtung quantitativer Methoden weiterentwickelt werden. Darüber hinaus können bestehende Maßnahmenstrategien (z. B. die NE-163-Checkliste) auf die speziellen Gegebenheiten der gemeinsamen Nutzung erweitert werden. Als mögliche Sicherungsmaßnahme bietet sich – neben einigen anderen – die Errichtung von „cyber-unabhängigen“ Abschalteinrichtungen (z. B. durch Wegschalten der elektrischen oder pneumatischen Hilfsenergie) an.

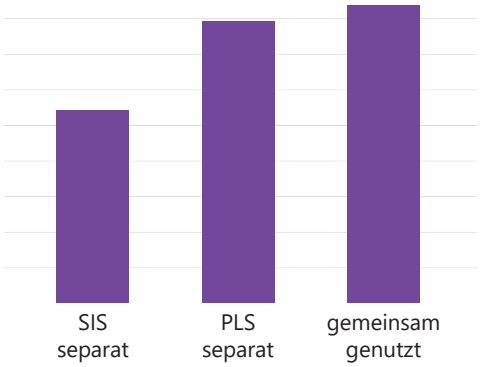

Abbildung 4: Cyberrisiko-Punktebewertung für Engineering-Station.

Darüber hinaus ist zu überlegen, welche Maßnahmen zur Kompensation des Mehrrisikos geeignet sind. Folgende Maßnahmenkategorien bieten sich an:

» Nutzung einer zusätzlichen – getrennten – Sicherheitsebene, etwa durch eine cyberunabhängige Abschaltung, z. B. elektrisch, pneumatisch oder mechanisch.

» Maßnahmen zur Stärkung von Trennung und Unabhängigkeit über z. B. unabhängige Benutzerinnen und Benutzer, eine Trennung der Datenhaltung, ein Vier-Augen-Prinzip

» Erhöhung der allgemeinen Cybersecurity (z. B. durch Multifaktor-Authentifizierung, stringente Steuerung der Kommunikationsverbindungen, aktives Vunerability- und Patchmanagement, etc.)

Dr. Felix Kahrau
anapur AG
67227 Frankenthal
f.kahrau@anapur.de

Erwin Kruschitz
anapur AG
67227 Frankenthal
e.kruschitz@anapur.de

Jan Russmann
Dow
21683 Stade
jrussmann@dow.com

Benedikt Bittcher
Wacker Chemie
81737 München
benedikt.bittcher@wacker.com

Detlef Winkel
Bayer AG
51368 Leverkusen
detlef.winkler@bayer.com