NAMUR - Interessengemeinschaft
Automatisierungstechnik der Prozessindustrie e.V.

AK-PRAXIS

Ethernet – APL – Security Advisory

Stand: 2025-01-20

AK 4.18.3 Automation Security

Verfasser: Detlef Winkel, Bayer
Lars Stephan Büldt, Tueg-Schillings
Emanuel Trunzer, BASF
Hartmut Manske, Merck
Bernd Renzing, Bayer
Daniel Kensik, Dow
Jan Russmann, Dow
Robin Krumm, Admeritia
Martin Floeck, BASF
Alexander Hainke, TH Köln
Alen Mahendrarajah, TH Köln
Paul David Sprengel, TH Köln
Sascha Kolanos, Bayer
Bert De Wilde, Exxon
Alexander Meurer
David De Bari, Exxon
Walter Speth, Bayer
Benedikt Bittcher, Wacker

AK-Leiter: Erwin Kruschitz, anapur

Diese AK-PRAXIS spiegelt die Erfahrungen der Mitglieder im AK 4.18 wider und ist im Rahmen des Arbeitskreises abgestimmt. Sie hat nicht den Konsensgrad einer NAMUR-Empfehlung oder eines NAMUR-Arbeitsblatts. Mit einer AK-PRAXIS hat der Arbeitskreis die Möglichkeit, zeitnah eigene Erfahrungen für interessierte Leser zur Verfügung zu stellen.

Vorwort

Diese AK-PRAXIS ist fokussiert auf den Bereich Cyber Security mit Bezug auf Ethernet-APL.
Als Umfeld wird eine Automatisierungsinfrastruktur für eine Anlage der Prozesschemie unterstellt.

Es wird angenommen, dass die Leserschaft aus Personal im betrieblichen Umfeld besteht. Es werden darunter auch IT-Administratoren angesprochen, allerdings nicht in dem Verständnis, dass es sich um Personen handelt, die eine qualifizierende Ausbildung im Fachgebiet „Information Technology“ erfahren haben und deren alleinige Aufgabe in der Systemadministration besteht. Insbesondere werden als Leserschaft keine Security-Experten angenommen.
Im Nachfolgenden werden konkrete Handlungsempfehlungen gegeben, wie übliche Aufgaben ausgeführt werden, sodass die Cyber-Security hinreichende Berücksichtigung findet, um dem aktuellen Stand der Technik zu entsprechen.

Inhaltsverzeichnis

1 Einleitung ... 3
2 Ziel ... 3
3 Anwendungsbereich ... 3
4 Normative Verweise ... 3
5 Begriffe und Definitionen ... 3
6 Betrachtetes System ... 5
7 Zusätzliche Betrachtungswinkel durch die Nutzung der Ethernet-APL-Technologie ... 5
7.1. Generell ... 5
7.2. Risiken im Vergleich zu “TAK” ... 5
8 Maßnahmen ... 7
8.1. Physische Sicherheit (Betreiber) ... 7
8.2. Netzwerksegmentierung (Betreiber) ... 7
8.3. Prozesse (Betreiber) ... 8
8.4. Schwachstellenmanagement (Betreiber / Hersteller) ... 8
8.5. Gerät ist updatefähig über den gesamten Lebenszyklus (Betreiber / Hersteller) ... 9
8.6. Gerät kann die Integrität der gespeicherten Daten gewährleisten (Hersteller) ... 9
8.7. Daten/Konfiguration sind sicher löschbar (Betreiber / Hersteller) ... 9
8.8. Logischer Zugriffsschutz und Härtung (Betreiber / Hersteller) ... 10
8.9. Erfassung von Systemzugriffen und -änderungen (Betreiber / Hersteller) ... 10
9 Chance ... 11

1 Einleitung

Ethernet Advanced Physical Layer (Ethernet-APL) ist eine Netzwerkinfrastruktur, welche auf die Anforderungen der Prozessindustrie zugeschnitten ist. Die Entwicklung von Ethernet-APL wurde durch das Bedürfnis nach breitbandiger Anbindung von Feldgeräten über relativ große Entfernungen sowie der gleichzeitigen Bereitstellung von Energieversorgung und Kommunikationssignalen über ein zweiadriges Kabel motiviert. Zudem ermöglicht es einen betriebssicheren Einsatz in explosionsgefährdeten Bereichen, teilweise unter Verwendung bereits vorhandener Verkabelungen.

Als Teil des weitverbreiteten Ethernet-Standards bietet Ethernet-APL ein hohes Maß an Robustheit für einen zuverlässigen Betrieb.

Im Bereich der Informationstechnologie ist Ethernet längst zur Standard-Kommunikationslösung geworden. “Industrial Ethernet” ist die gängige Bezeichnung für Varianten dieses Standards für die Fertigungs- und Prozessindustrie. Ethernet-APL wurde, als die bisher fehlende Verbindung ins Feld entwickelt und erweitert die vereinheitlichte Ethernet-Kommunikation bis hin zur Feldinstrumentierung. Es soll sowohl die traditionelle 4-20 mA-Anbindung und Feldbusse z. B. PROFIBUS oder Foundation Fieldbus, als auch HART in Zukunft ablösen.

2 Ziel

Diese Empfehlung beschreibt Realisierungsmöglichkeiten von Ethernet-APL-Installationen unter den Gesichtspunkten der IT/OT-Security.

3 Anwendungsbereich

Diese Empfehlung gilt für Ethernet-APL-Installationen, die in der Prozessindustrie in bestehenden, aber auch in Neuanlagen eingesetzt werden.

Dieses Dokument basiert auf der einschränkenden Annahme, dass in den Betrieben der Prozesschemie das PROFINET-Protokoll über Ethernet-APL zum Einsatz kommt.

Dieses Dokument richtet sich sowohl an Anwender, vor allem Ingenieure (nicht IT/OT-Security-Spezialisten) und Planer, als auch Hersteller.

Die Nutzung von APL in Anwendungen der funktionalen Sicherheit wird bei der Erstellung dieses Dokuments (Dezember 2024) nicht betrachtet. Dies liegt im Wesentlichen an den derzeit nicht verfügbaren Komponenten mit entsprechender Zulassung und Zertifizierung. Für den Einsatz von Ethernet-APL für funktionale Sicherheit sollten zusätzliche Anforderungen/Assessments wie z.B. gemäß NA 163 beachtet werden.

4 Normative Verweise

Die folgenden zitierten Dokumente (in der jeweils gültigen Fassung) sind für die Anwendung dieses Dokuments hilfreich. In diesen Dokumenten finden sich relevante Hinweise zum Verständnis und zur Anwendung dieses Dokuments.

- Relevante Teile der IEC 62443
  - - 2-1 v2.0 für Betreiber / -2-4 Edition 1.1, August 2017
  - - 3-2 Edition 1.0, Juni 2020 Integratoren / 3-3 Edition 1.0, August 2013
  - - 4-1 2018 / -4-2 2019 Produkthersteller
- NA163 Ed. 2024
- IT-Grundschutz des BSI 2023

5 Begriffe und Definitionen

Die in diesem Dokument genutzten Begriffe werden auf Grundlage des BSI-Grundschutz Stand 2023 genutzt und kontextspezifisch angepasst / vereinfacht, und um spezifische Begriffe ergänzt, um ein gemeinsames Verständnis zu schaffen:

Asset: In diesem Dokument bezieht sich "Assets" auf alle technischen und infrastrukturellen Komponenten, die in der Automatisierung und Prozesssteuerung verwendet werden.

Ethernet-APL (Advanced Physical Layer) beschreibt die OSI-Layer-1-Schicht für Single-Pair-Ethernet, über die Protokolle der höheren Schichten 2 bis 7 übertragen werden können.

Traditionelle Anlagen-Kommunikation (im weiteren Verlauf “TAK”) ist die Übertragung mittels Stromschleifen (i.d.R. 4-20 mA) zwischen Sensor/Aktor und CPU (mit oder ohne HART) oder Feldbusprotokolle.

Bedrohung (englisch „threat“) Ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen oder Systemen beeinträchtigen **kann**, wodurch der Person, die die Informationen besitzt oder benutzt, ein Schaden entstehen kann.

Exploit ist ein Programm oder ein Code, der gezielt eine **Schwachstelle** ausnutzt, um unbefugten Zugriff zu erlangen oder um Schaden anzurichten. Ein Exploit ist also das Mittel, mit dem eine Schwachstelle ausgenutzt wird.

Gefahr ist übergeordneter Begriff, wohingegen eine „Gefährdung“ eine genaue beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) darstellt. Die Gefahr ist beispielsweise ein “Datenverlust”, die Gefährdung wäre dann “defekter Datenträger”

Risiko wird definiert als die Kombination aus der Häufigkeit/Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens.
Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln.

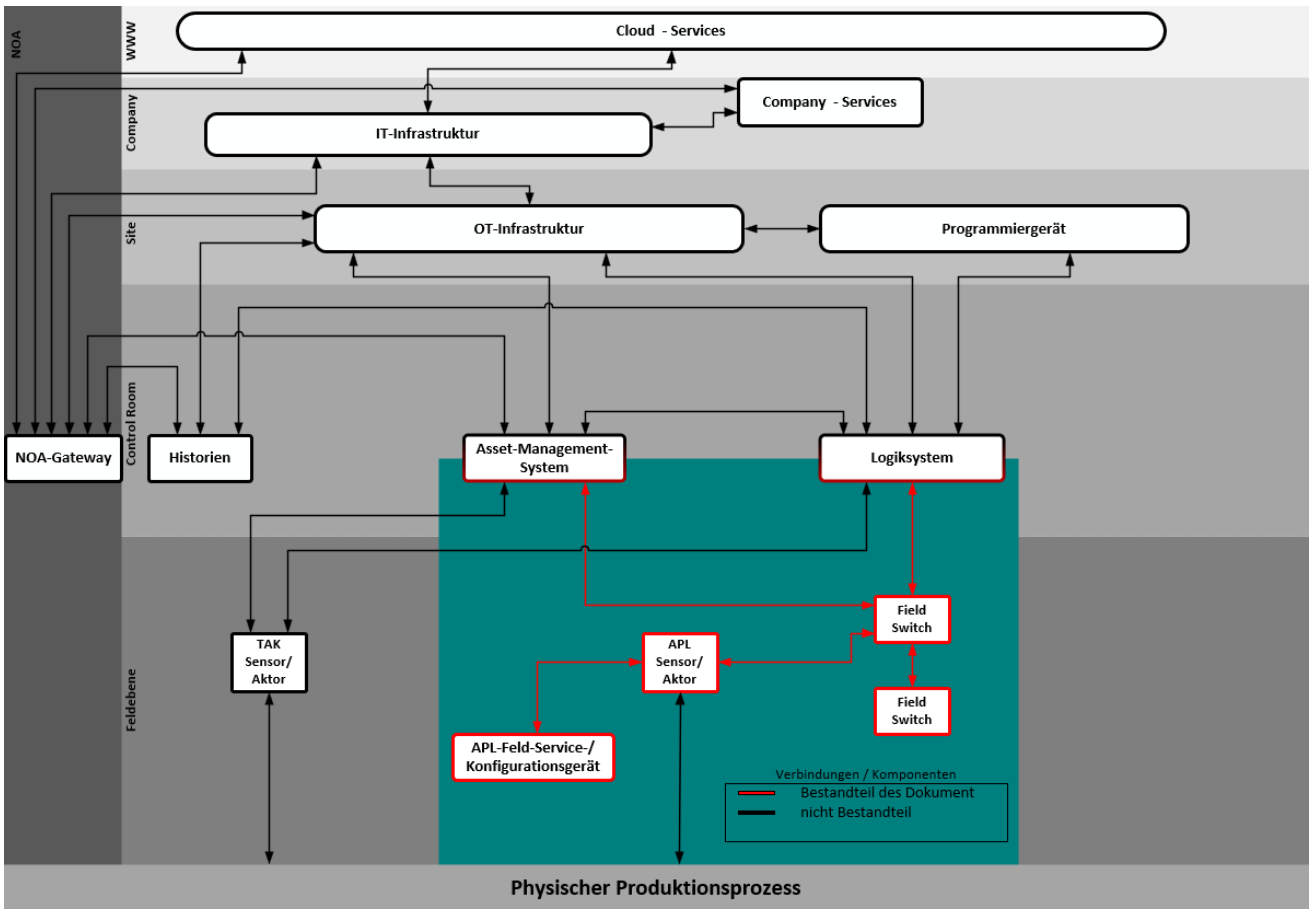
Schaden / Konsequenz: Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden“ genannt). Hierbei kann es sich grundsätzlich um eine positive oder negative Abweichung handeln, in diesem Dokument wird jedoch von der negativen Möglichkeit ausgegangen.

Schwachstelle (englisch „vulnerability“) Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines Systems, einer Anlage oder einer Institution. Ursachen können **technisch oder organisatorisch bedingt sein**. Eine Schwachstelle kann dazu führen, dass eine **Bedrohung** wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
Beispiel: Drei Dinge müssen zusammenkommen: Einbrecher (Bedrohung/Threat Actor) x Fenster (Schwachsteller/Vulnerability) x Brecheisen (Exploit)

Zugang Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme oder System-Komponenten und Netze zu nutzen.
Zugriff Mit Zugriff wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

6 Betrachtetes System



Betrachtetes System Bild 1

Es werden in diesem Dokument nur die Kernkomponenten der Ethernet-APL-Technologie betrachtet (siehe rot markierte Objekte in Zeichnung „Betrachtetes System Bild 1 1“)

Alle weiteren Komponenten werden über andere Prozesse als bereits genügend gesichert angesehen.

Sofern der Einsatz von Ethernet-APL in Einrichtungen der funktionalen Sicherheit (PLT-BS + SIL1-SIL3) geplant ist, muss der erhöhte Schutzbedarf, der sich durch die höheren Auswirkungen eines SIF ergeben kann, bei einer Risikoanalyse für diese Anwendung angemessen berücksichtigt werden. Z.B. die NA163 gibt hier mögliche Ansätze vor.

7 Zusätzliche Betrachtungswinkel durch die Nutzung der Ethernet-APL-Technologie

7.1. Generell

Die technologischen Unterschiede zwischen APL und traditioneller Anlagen-Kommunikation (TAK) machen die Durchführung einer zusätzlichen IT/OT Risikoanalyse notwendig.
Es ergeben sich durch die verwendeten Technologien neue Risiken und Chancen-im Vergleich zu TAK.

In einer Risikoanalyse wird, der aus einer Ausnutzung der unten gelisteten Schwachstellen resultierende Schaden bewertet, das Risiko bestimmt und gegebenenfalls kompensierende Maßnahmen definiert.

7.2. Risiken im Vergleich zu “TAK”

Aus der IT-Security-Perspektive gibt es mehrere Gründe, warum im Vergleich zur TAK zusätzliche Risiken mit Ethernet-APL verbunden sind:

1. **Vergrößerte Angriffsfläche**:

- Ethernet-APL ist eine digitale Kommunikationsschnittstelle, mit der Standard-Ethernet/IP -basierte Netzwerke errichtet werden. Diese stärkere Vernetzung über etablierte Protokolle stellt eine zusätzliche Angriffsoberfläche dar und eröffnet Möglichkeiten für Cyberangriffe, wie Spoofing von Daten, Denial-of-Service-Angriffe, Malware und andere digitale Bedrohungen, die bei TAK nicht vorhanden sind. Auch die stärkere und einfachere Vernetzung zu anderen Systemen können zusätzliche Maßnahmen erfordern.

  Zusätzlich kann diese Vernetzung dazu führen, dass unbeabsichtigt Änderungen an Netzwerkteilnehmer stattfinden, die zu einem Risiko führen können.

2. **Netzwerkverbindungen**:
   - Ethernet-APL-Komponenten bilden Netzwerke, d.h. sie sind potenziell anfällig für netzwerkbasierte Angriffe. Angreifer könnten versuchen, in das Netzwerk einzudringen, um auf kritische Systeme und Daten zuzugreifen.
3. **Komplexität der Systeme**:
   - Digitale Systeme sind oft komplexer als analoge Systeme, was bedeutet, dass sie mehr potenzielle Schwachstellen aufweisen. Die Vielzahl an Komponenten, Protokollen und Software kann zu Fehlkonfigurationen führen, die potenzielle Sicherheitsrisiken darstellen oder es aufwendiger machen Schwachstellen zu finden.
   - Eventuell einzusetzende Security Komponenten / Schutzmaßnahmen machen die Verwaltung des Gesamtsystems und Wartung komplexer.
4. **Abhängigkeit von Software/Firmware**:
   - Ethernet-APL-Systeme sind von Firmware abhängig, die bei sicherheitsrelevanten Änderungen aktualisiert und gewartet werden sollten.
   - Bei Bekanntwerden einer Security-relevanten Schwachstelle und Mitigation ist eine Erwägung der Notwendigkeiten des richtigen Installationszeitpunkts durchzuführen. Der Zeitpunkt der Schwachstellenbehandlung sollte die Kritikalität der Schwachstelle und des Betriebszustands berücksichtigen.
     Diese Abhängigkeit kann Sicherheitsanfälligkeiten mit sich bringen, insbesondere wenn Patches und Updates nicht rechtzeitig angewendet werden. Das Einspielen der Patches und Updates selbst kann auch eine Schwachstelle darstellen.
5. **Datenübertragung und -manipulation**:
   - Digitale Signale können einfacher während der Übertragung abgefangen, manipuliert oder gefälscht werden. Dies stellt ein Risiko für die Verfügbarkeit, Integrität und Vertraulichkeit der Daten dar.
6. **Zugriffs- und Identitätsmanagement**:
   - In digitalen Systemen ist ein Management notwendig, um sicherzustellen, dass nur autorisierte Benutzer, Geräte und Dienste auf das System zugreifen können.
   - Die technische Realisierung kann herausfordernd sein, der Stand der Technik sollte fortlaufend beobachtet werden.
8. **Sicherheitsvorfälle und -reaktionen**:
   - Bei einem Sicherheitsvorfall in einem Ethernet-APL-System kann die Reaktion komplexer und zeitaufwändiger sein, da die Ursachen möglicherweise schwieriger zu identifizieren sind und mehrere Systeme betroffen sein können.

Zusammenfassend lässt sich sagen, dass APL aus der IT-Security-Perspektive mehrere Risiken birgt, die in der TAK nicht oder weniger ausgeprägt vorhanden sind. Die stärkere Vernetzung unter Verwendung von Standard-Ethernet/IP-Kommunikation und die dadurch bedingte größere Angriffsfläche + die größere Abhängigkeit von Software erhöhen die Wahrscheinlichkeit von Sicherheitsanfälligkeiten und -vorfällen. Daher ist es wichtig, geeignete Sicherheitsmaßnahmen zu implementieren, um diese Risiken zu minimieren.

Trotz der nennenswerten Risiken ergeben sich bei fachgerechter Umsetzung auch eine Vielzahl von Chancen durch die Anwendung von APL.

8 Maßnahmen

8.1. Physische Sicherheit (Betreiber)

Erklärung

Durch die Möglichkeit, dass bei einer Verbindung zu einem Feldgerät oder Switch im Feld, im Gegensatz zur TAK, eine Vielzahl von Ethernet-APL-Geräten über das Netzwerk erreicht werden kann, ist ein höherer physischer Schutz der Feldgeräte, vor allem der Switche, erforderlich. Ist kein physischer Schutz zu gewährleisten, müssen andere Maßnahmen ergriffen werden.

Maßnahmen

8.1.1 SWITCHE und andere Netzwerkkomponenten (nicht Sensoren und Aktoren)

- Idealerweise wird der physische Schutz durch robuste Schränke realisiert, die mit Schließsystemen von angemessener Qualität (=Schutz) ausgestattet sind. Prozesse zur Benutzerverwaltung sind erforderlich, Standardschließungen sollten vermieden werden.
- Alternativ oder zusätzlich sollte die Tür/Klappe überwacht werden und jedes Öffnen sollte eine Meldung im Leitsystems auslösen (=Detektion).
- Wenn beides nicht möglich ist oder technisch zu aufwendig, können die Schränke alternativ mit Sicherheitssiegeln versiegelt werden, die beim Entfernen irreversibel beschädigt werden. Hierzu ist ein Prozess für eine regelmäßige Überprüfung zu definieren.
- Alternativ und ergänzend können nicht verwendete Anschlüsse (z.B. RJ45-Schnittstellen) mit mechanischen Schlössern gesichert werden.

Hinweis: Angemessene Maßnahmen, die einen gleichwertigen logischen Zugriffsschutz und Überwachung sind zu berücksichtigen.

Die getroffenen Schutzmaßnahmen sollten dem Schutzbedarf der erreichbaren Teilnehmer entsprechen. (Wenn SIFs theoretisch erreichbar wären, sollte i.d.R. ein höheres Schutzniveau umgesetzt werden)

8.1.2 Sensoren und Aktoren

- Nicht verwendete Anschlüsse (z.B. Push-in Konnektoren, RJ45-Schnittstellen, Serviceschnittstellen) mit mechanischem Zugriffsschutz sichern.
- Bei erhöhtem Schutzbedarf sind Sicherheitssiegel zu verwenden, die beim Entfernen irreversibel beschädigt werden.

Hinweis: Angemessene Maßnahmen zum logischen Zugriffsschutz und Überwachung sind zu berücksichtigen.

8.1.3 Verdrahtung und Verbindungen

- Stichleitungen zu abgelegene Feldgeräten oder anderen APL-Komponenten außerhalb des gesicherten Bereichs, zum Beispiel in abgesetzten Tanklagern, sind besonders manipulationsgefährdet und sollten daher in geeigneter Weise – unter Berücksichtigung des Gefährdungspotentials der Anbindung -- gegen physische Manipulationen gesichert werden, z. B. in sicheren Kabelkanälen oder durch Verwendung manipulationssicherer Kabel.

8.1.4 AMS, BPCS-Logiksystem und Servicegeräte

- Der **Zugang** sollte nur autorisiertem Personal gestattet sein.

8.2. Netzwerksegmentierung (Betreiber)

Erklärung

Die Segmentierung der Netzwerkarchitektur ist eine bewährte Methode zur Verbesserung der IT-Sicherheit in Automatisierungsnetzwerken. Geräte können dabei nach Kriterien wie Standort, funktionaler Kritikalität, Schutzbedarf, Vertrauensstufe oder anderen Anforderungen in separate Segmente unterteilt werden. Ein

segmentiertes Netzwerk ist widerstandsfähiger gegen Cyber-Angriffe, da eine Kompromittierung in der Regel auf das betroffene Segment begrenzt bleibt. Zur Sicherstellung der logischen Trennung zwischen den Segmenten wird die zonenübergreifende Datenkommunikation häufig durch uni- und bidirektionale Gateways, Switches, Router, Firewalls oder Datendioden geregelt. Neben diesen hardwarebasierten Lösungen können auch softwarebasierte Ansätze zur Segmentierung eingesetzt werden.

Maßnahmen

- Der Übergang zwischen Netzsegmenten sollte mittels definiertem Zonenübergang realisiert werden, der dem Zielschutzniveau des Netzsegmentes entspricht. Der Übergang zwischen Netzsegmenten ohne Sicherheitskomponente ist zu unterbinden.
- Eine dauerhafte Kommunikation zum AMS oder anderen Teilnehmern, die auf mehrere unabhängigen Segmente zugreifen können, sollte nicht erlaubt sein. Eine Ausnahme bildet das BPCS-Logiksystem oder andere Komponenten, die zwingend dauerhaft verbunden bleiben müssen.

  Hier sollte eine dedizierte Zuschaltung, z.B. über einen Schlüsselschalter, nur bei Bedarf erfolgen oder über andere technische Möglichkeiten ein sicherer Betrieb sichergestellt sein.
- Der Austausch von Prozessdaten (zyklische Kommunikation via PROFINET) zwischen dem AMS und den Feldgeräten sollte technisch unterbunden werden. Das AMS sollte lediglich über Protokolle, die zur Konfiguration der Ethernet-APL-Geräte dienen, mit diesen kommunizieren können.
- Ethernet-APL-Netzringe sollten logisch und physisch voneinander isoliert sein.
- BPCS-Logiksysteme sollten keinen Datenverkehr zwischen Ethernet-APL-Ringen weiterleiten oder das Ethernet-APL-Netzwerk mit anderen Netzwerksegmenten verbinden (d. h. als Gateway zwischen dem Anlagennetzwerk oder Terminalnetzwerk und dem APL-Netzwerk fungieren).
- Die Begrenzung der Anzahl der Feldgeräte pro Ring reduziert die Angriffsfläche für den Fall, dass ein Gerät oder die Netzwerkinfrastruktur kompromittiert wird. Daher ist eine gute Segmentierung -- zum Beispiel pro Teilanlage -- ein guter und effektiver Schutz.

8.3. Prozesse (Betreiber)

Erklärung

Durch die höhere Komplexität der APL-Feldsysteme, wie zum Beispiel umfangreiche Netzwerke, Anzahl der Geräte, Firmwarestände und Updates, ist es wichtig Prozesse zu definieren und zu dokumentieren, die den gesamten Lebenszyklus der Komponenten beschreiben. Dies hilft im täglichen Gebrauch der Komponenten, aber auch im Schadensfall, Schulung und Dokumentation gegenüber Dritten.

Hier kann oftmals auf vorhandene und etablierte Prozesse aufgesetzt werden.

Maßnahmen

- Es sollte eine Übersicht aller Geräte mit den wichtigsten Daten, wie Gerätetyp, IP-Adresse, Firmwarestand, Patchstand, etc. verfügbar sein.
- Prozesse für Beschaffung, Inbetriebsetzung, produktive Verwendung, Ausserbetriebsetzung, Verhalten im Schadensfall, etc. sollen verfügbar sein.
- Eine Vorgehensweise zu allen Maßnahmen zur Erhöhung der IT/OT-Sicherheit sollten beschrieben sein.
- Das Personal sollte über die Prozesse informiert und geschult sein

8.4. Schwachstellenmanagement (Betreiber / Hersteller)

Erklärung

Durch das Schwachstellenmanagement der Hersteller wird sichergestellt, dass Ethernet-APL-Geräte gegen bekannte Bedrohungen geschützt sind und neue Sicherheitslücken schnell geschlossen werden, um die Integrität und Sicherheit der Systeme zu gewährleisten.

Maßnahmen

- Hersteller bieten Schwachstellenmanagement-Dienste an. Schwachstellen werden zeitnah kommuniziert, um diese zu bewerten zu können. Sicherheitsupdates sowie Patches werden bereitgestellt.
- Auf Anwenderseite müssen Prozesse etabliert sein, um die Erkennung neuer Sicherheitsupdates und deren Installation über den gesamten Lebenszyklus in den betroffenen Komponenten sicherzustellen.
- Für den Bezug von Firmwareupdates sollten ausschließlich die vom Hersteller zur Verfügung gestellten Bezugsquellen dienen und eine Integritätsprüfung durchgeführt werden, z.B. mittels Überprüfung von Hashes oder digitalen Signaturen.
- Darüber hinaus sollte die Firmware umfassend in Offline- oder Testumgebungen getestet werden, um sicherzustellen, dass sie keine Sicherheitsrisiken oder Fehler aufweist. Für die Durchführung ist idealerweise der Hersteller verantwortlich.

8.5. Gerät ist updatefähig über den gesamten Lebenszyklus (Betreiber / Hersteller)

Erklärung

Geräte sollen über ihren gesamten Lebenszyklus hinweg updatefähig sein, um zu gewährleisten, dass das Gerät während seiner gesamten Nutzung sicher und in einem mangelfreien Zustand bleibt, indem es regelmäßig neue Stabilitäts- und Sicherheitsupdates erhält. Dies sollte vom Hersteller sichergestellt sein und technisch auf einfachem Wege und im Idealfall ohne die Notwendigkeit des Abschaltens des Gerätes während des Updateprozesses sichergestellt sein. Es sollte erkennbar sein, ob es sich um ein Security- oder ein funktionales Update handelt. Ein Verschmelzen beider Updates sollte vermieden werden und Security-Updates sollten abwärtskompatibel sein.

Updates müssen ausreichend dokumentiert sein, so dass diese auch im regulierten Umfeld (pharmazeutische Industrie) verwendet werden können.

Maßnahmen

- Hierfür ist ein Prozess vom Betreiber zu etablieren, der sicherstellt, dass über den kompletten Lebenszyklus hinweg die Security-Anforderungen erfüllt und Updates in die Geräte eingebracht werden. Dies umfasst Beschaffung, Betrieb, Wartung, Inbetriebnahme, Außerbetriebnahme und Entsorgung. Dies ist in ausreichendem Maße zu dokumentieren.

8.6. Gerät kann die Integrität der gespeicherten Daten gewährleisten (Hersteller)

Erklärung

Die Integrität der Daten soll gewährleistet sein, um ein zufälliges oder gewolltes Ändern dieser zu vermeiden.

Maßnahmen

- Das Gerät verwendet Mechanismen wie Prüfziffern, Hashes oder digitale Signaturen, um sicherzustellen, dass die gespeicherten Daten während der Speicherung oder Übertragung nicht manipuliert oder beschädigt werden.
- Im Idealfall sollen Geräte ausgewählt werden, die über ausreichende Hardware-Ressourcen verfügen, um zukünftige erweiterte Sicherheitsfunktionen wie kryptografische Verschlüsselung und Firmware-Updates während der gesamten Produktlebensdauer implementieren zu können, sobald diese verfügbar sind.

8.7. Daten/Konfiguration sind sicher löschbar (Betreiber / Hersteller)

Erklärung

Da es sich bei Ethernet-APL-Geräten um digitale Geräte handelt und diese dieselben Informationen wie Standard-IT-Geräte (IP-Adresse, MAC-Adresse, etc.) enthalten, sind bei der Ausserbetriebsetzung, Reparatur und Verschrottung gleiche oder ähnliche Prozesse einzusetzen.

Maßnahmen

- Eventuelle Datenträger sind zu entfernen und vertrauliche Daten, wenn vorhanden, sicher zu löschen.

- Das Gerät ist gezielt auf Werkseinstellung zurückzusetzen. Dabei ist die sichere Löschung der ursprünglichen Parametrierung zu gewährleisten.

8.8. Logischer Zugriffsschutz und Härtung (Betreiber / Hersteller)

Erklärung

Die Geräte sollten vor unberechtigtem Zugriff geschützt werden. Diesbezüglich ist im Umfeld von Ethernet-APL vor allem zu beachten, dass durch den Zugang zu einem Gerät, über Standard-Netzwerkdienste, auch weitere Geräte erreicht werden können. werden können. Hier sind neben den Feldkomponenten auch die entsprechenden Applikationen des AMS und den Servicegeräte zu betrachten.

Maßnahmen

- Änderung von Standardpasswörtern (auch für Feldgeräte)
- Deaktivierung von nichtverwendeten Ports
- Deaktivierung ungenutzter Dienste, z.B. embedded-Web Server, sind zu deaktivieren, falls bzw. sobald sie nicht mehr benötigt werden.
- Verwendung angemessen starker Passwörter
- Wenn technisch möglich, die vorübergehende Sperrung der Schnittstelle nach erfolglosen Anmeldeversuchen.
- Nicht verwendete Protokolle/Dienste sollten deaktiviert werden (z. B. SSH, SNMP, wenn nicht benötigt).
- Wenn möglich, sind sichere Protokolle zu verwenden, z. B. https anstelle von http
- Standardkonten sind zu löschen oder zu deaktivieren
- Der Zugriff auf das Gerät darf nur mit angemessener Authentifizierung/Autorisierung möglich sein.
- Link-Up/Down-Ereignisse (Verbindung / Trennung von Komponenten) sollten eine Alarmierung auslösen.
- PC-basierte Komponenten (AMS und Servicegeräte) sollten nach den Vorgaben gehärtet sein (zum Beispiel nach BSI-Grundschutz und/oder eigenen Regularien des Betreibers)
- Falls unterstützt, sollten applikationsbedingte rollenbasierte Zugriffe und personalisierte Konten verwendet werden.
- Security-Funktionen der Geräte, vor allem der Switche, sollten aktiviert werden. Dies können z.B. Bandbreitenlimitierungen oder der Schutz vor Denial-of-Service-Angriffen sein.

8.9. Erfassung von Systemzugriffen und -änderungen (Betreiber / Hersteller)

Erklärung

Die Protokollierung von Ereignissen ist entscheidend, um Fehler oder sicherheitsrelevante Vorfälle frühzeitig zu erkennen. Alle Zugriffe (auch erfolglose) auf das System sollten systematisch protokolliert werden, um unberechtigte Zugriffsversuche aufzudecken und zu analysieren. Diese Protokolle ermöglichen eine detaillierte Überprüfung der Systemaktivitäten und helfen, potenzielle Sicherheitsprobleme zeitnah zu identifizieren und zu beheben.

Maßnahmen

- Zugriffe und Änderungen protokollieren (standardmäßig zu aktivieren)
- Es sollten mindestens der Zeitpunkt, das eingesetzte Benutzerkonto und die Art der Änderung protokolliert werden.
- Es sollten Prozesse etabliert werden, diese Logs auszuwerten und bei Bedarf zu reagieren.

9 Chancen

Der Einsatz von APL wirkt als Enabler oder essenzielle Grundlage für Anwendungen die höhere Ansprüche an Datenmenge und Durchsatz haben.

- Bessere Analysemöglichkeiten durch höhere Bandbreite
- Zugriffsverfolgung und Nachverfolgung
- Rollen- und Rechtemanagement
- Änderungsmanagement
- Assetmanagement Anbindung an zentraler Stelle
- Durchgängige Technologie
- Nutzung etablierter Security Prozesse