Sicherheit im System.
Schutz für Mensch und Maschine.

CYBERSECURITY
MANUAL FIELD DEVICES

SCHMERSAL
THE DNA OF SAFETY

INHALT

ALLGEMEINE INFORMATIONEN

CYBERSECURITY IM INDUSTRIELLEN UMFELD

Cybersecurity bezeichnet den Schutz industrieller Automatisierungs- und Steuerungssysteme (IACS) vor unbeabsichtigten oder vorsätzlichen Beeinträchtigungen der Verfügbarkeit, Integrität und – soweit relevant – der Vertraulichkeit von Daten und Funktionen.
Im industriellen Umfeld basiert Cybersecurity auf einem ganzheitlichen Ansatz aus technischen, organisatorischen und physikalischen Maßnahmen und orientiert sich an der Normenreihe IEC 62443.

CYBERSICHERHEITSKONZEPT

Zum Schutz vor Cybersicherheitsbedrohungen muss der Betreiber über ein umfassendes Cybersicherheitskonzept verfügen, das kontinuierlich überwacht und gepflegt werden muss. Ein geeignetes Konzept umfasst organisatorische, technische, verfahrenstechnische, elektronische und physischen Verteidigungsebenen und berücksichtigt geeignete Maßnahmen für verschiedene Arten von Risiken.
Die in diesem Produkt implementierten Maßnahmen können den Schutz vor Cybersicherheitsbedrohungen nur dann unterstützen, wenn das Produkt als Teil eines solchen Konzepts eingesetzt wird.

Weitere Informationen finden Sie unter **www.schmersal.com\cybersecurity**

- Allgemeine Informationen zur Cybersicherheit
- Kontaktmöglichkeit zur Meldung von Schwachstellen
- Informationen zu bekannten Schwachstellen (Sicherheitshinweise)

SECURITY KONTEXT

Physische Umgebung

- Das Produkt ist nicht vorgesehen für die Verwendung in einfach zugänglichen Bereichen. Der Anwender muss sicherstellen, dass das Produkt vor unbefugten Zugriff geschützt ist.
- Beschränken Sie den physischen Zugang zum Gerät und der Verkabelung. Dazu gehört beispielsweise ein verschlossener Schaltschrank oder ein beschränkter Zugang zu den Räumen, in denen das Produkt betrieben wird.
  Nur autorisiertes Personal sollte Zugang haben.
- Schützen Sie das Produkt und Ersatzteile gegen unbefugten Zugriff auch während Transport und Lagerung, um Manipulation vorzubeugen.

Netzwerk

- Der Anwender muss sicherstellen, dass alle Netzwerke, mit denen das Gerät verbunden ist, vertrauenswürdig sind (segmentierte Netzwerke mit Firewall).
- Fernzugriff durch unbefugte Personen oder physischer Zugriff auf Geräte durch unbefugte Personen ist durch Zugriffsbeschränkungen und organisatorische Maßnahmen zu verhindern.

ORGANISATORISCHE MAßNAHMEN

Social-Engineering, d. h. unbefugte Personen gewinnen das Vertrauen von berechtigten Personen, ist durch organisatorische Maßnahmen und Sensibilisierung der Mitarbeiter zu verhindern.

BEKANNTE SCHWACHSTELLEN

Zum Zeitpunkt der Risikoanalyse und des Inverkehrbringens weist das Produkt keine bekannten, relevanten Schwachstellen auf, die von unbefugten Benutzern ausgenutzt werden könnten.
Die Risikoanalyse wird regelmäßig aktualisiert, um etwaige neue Risiken oder Schwachstellen zu berücksichtigen, die bekannt werden. Verbleibende Risiken müssen durch die in der Produktdokumentation beschriebenen Maßnahmen sowie durch ein umfassendes Cybersicherheitskonzept reduziert werden.

VORSICHTSMAßNAHMEN

Trotz aller Abwehrmaßnahmen kann es dennoch vorkommen, dass Unbefugte das System kompromittieren.

- Es sollten geeignete Vorkehrungen für die gesamte Systemumgebung getroffen werden, damit die Systemumgebung nach einem Vorfall so schnell wie möglich wieder in Betrieb genommen werden kann.
- Achten sie auf vertrauenswürdige Quellen, wenn sie das Produkt erwerben.
- Prüfen Sie die Verpackung und das Gerät auf Beschädigungen. Verletzte Siegel oder Kratzer am Gerät könnten auf eine Manipulation hindeuten.

VORHERSEHBARE FEHLANWENDUNG

Zur Reduzierung von Risiken und zur Erhaltung der Integrität sind die folgenden Punkte nicht zulässig

- Verbindung mit unsicheren Netzwerken.
- Aktivieren von Services und Ports die nicht für den Betrieb benötigt werden.
- Ständige Verbindung einer Konfigurationssoftware mit dem Produkt.
- Betrieb des Produkts in einem ungesicherten Bereich.

UPDATES

Je näher ein Gerät an der Prozessebene (Level 0) eingesetzt wird und je einfacher die Kommunikationsschnittstelle ist, desto stärker verlagert sich Cybersecurity von der Protokollebene auf die Systemarchitektur und den physischen Schutz. Sicherheitsrelevante Updates beziehen sich daher auf Geräte, die unmittelbar mit einem Ethernet basierten Netzwerk verbunden sind. Die hier aufgeführten Feldgeräte verfügen über keine Netzwerkschnittstelle. Updates an diesen Geräten sind nur im Servicefall notwendig und können nur von der Firma Schmersal durch speziell geschultes Personal mit spezieller Hardware und Software durchgeführt werden. Firmware Version und Konfigurationsdaten werden werksseitig bei der Firma Schmersal und im Gerät gespeichert.

HAFTUNGSAUSSCHLUSS

Der Anwender ist verantwortlich für die ordnungsgemäße Umsetzung der empfohlenen Maßnahmen
- Schulung und Sensibilisierung von Mitarbeitenden
- Einhaltung gesetzlicher und regulatorischer Anforderungen

Eine Haftung wird – soweit gesetzlich zulässig – ausgeschlossen für:
- mittelbare Schäden, Folgeschäden oder entgangenen Gewinn
- Schäden infolge nicht umgesetzter oder verspätet umgesetzter Empfehlungen
- Sicherheitsvorfälle, die außerhalb des definierten Leistungsumfangs liegen
- Angriffe, die trotz normkonformer Umsetzung der Maßnahmen erfolgen

Unberührt bleiben Haftungsansprüche aus Vorsatz oder grober Fahrlässigkeit.

IO-LINK / IO-LINK SAFETY DEVICES

SYSTEMCHARAKTERISTIK

- Standardisierte kabelgebundene Punkt-zu-Punkt-Kommunikation gemäß IEC 61131-9
- Keine Netzwerkfunktionen (kein Routing, keine IP-Adressierung)
- Typischer Einsatz auf IEC-62443-Level 0 (Feldebene)
- Kommunikation ausschließlich zwischen Device und Master

PROTOKOLLSEITIGE SECURITY-EIGENSCHAFTEN

IO-Link stellt keine klassischen Cybersecurity-Funktionen bereit:

- keine Verschlüsselung
- keine Authentifizierung
- keine Zugriffskontrolle
- lediglich einfache Integritätsprüfungen (z. B. CRC)

Diese Einschränkungen sind protokollbedingt und bewusst gewählt, um eine einfache, robuste Feldkommunikation zu ermöglichen.

SCHUTZZIELE UND RISIKOBEWERTUNG (IEC-62443-ORIENTIERT)

Schutzziel	Risikobewertung	Begründung
Verfügbarkeit	hoch	Unterbrechung der physischen Verbindung führt unmittelbar zum Funktionsverlust
System- & Datenintegrität	hoch	Manipulation kann Prozesswerte verfälschen
Vertraulichkeit	niedrig	Sniffing nur bei physischem Zugriff mit Spezialhardware
Authentifizierung / Zugriffskontrolle	nicht zutreffend	Keine Benutzerinteraktion auf Device-Ebene

BEDROHUNGSMODELL

Relevante Bedrohungen entstehen ausschließlich bei Verletzung der physischen Sicherheitszone:

- Unterbrechen der IO-Link-Leitung (Denial of Service)
- Manipulation von Parametern oder Gerät
- Einschleusen eines manipulierten Geräts
- Abgriff von Diagnosedaten
- Sniffing oder Datenmanipulation mit Spezialhardware

HANDLUNGSEMPFEHLUNGEN FÜR IO-LINK-DEVICES

Physischer Schutz

Schutz von Gerät, Leitung und Steckverbindungen vor unbefugtem Zugriff

- Einbau in geschützten Bereichen oder verschließbaren Schaltschränken
- Anwendung organisatorischer Zugriffsregeln

System- und Zonenkonzept

- Integration in eine definierte Sicherheitszone gemäß IEC 62443-2-1
- Keine direkte Exposition zu ungeschützten Bereichen

Betrieb und Wartung

- Nutzung von Backup-&-Restore / Restore
- Überwachung gemeldeter Ereignisse
- Befolgung von Hersteller-Security-Hinweisen

Bewertung nach MVO

Die nachfolgende schematische Darstellung zeigt, wie das Gerät nach der DIN EN50742 im System eingebunden werden sollte, um den Schutz vor Korrumpierung zu gewährleisten:

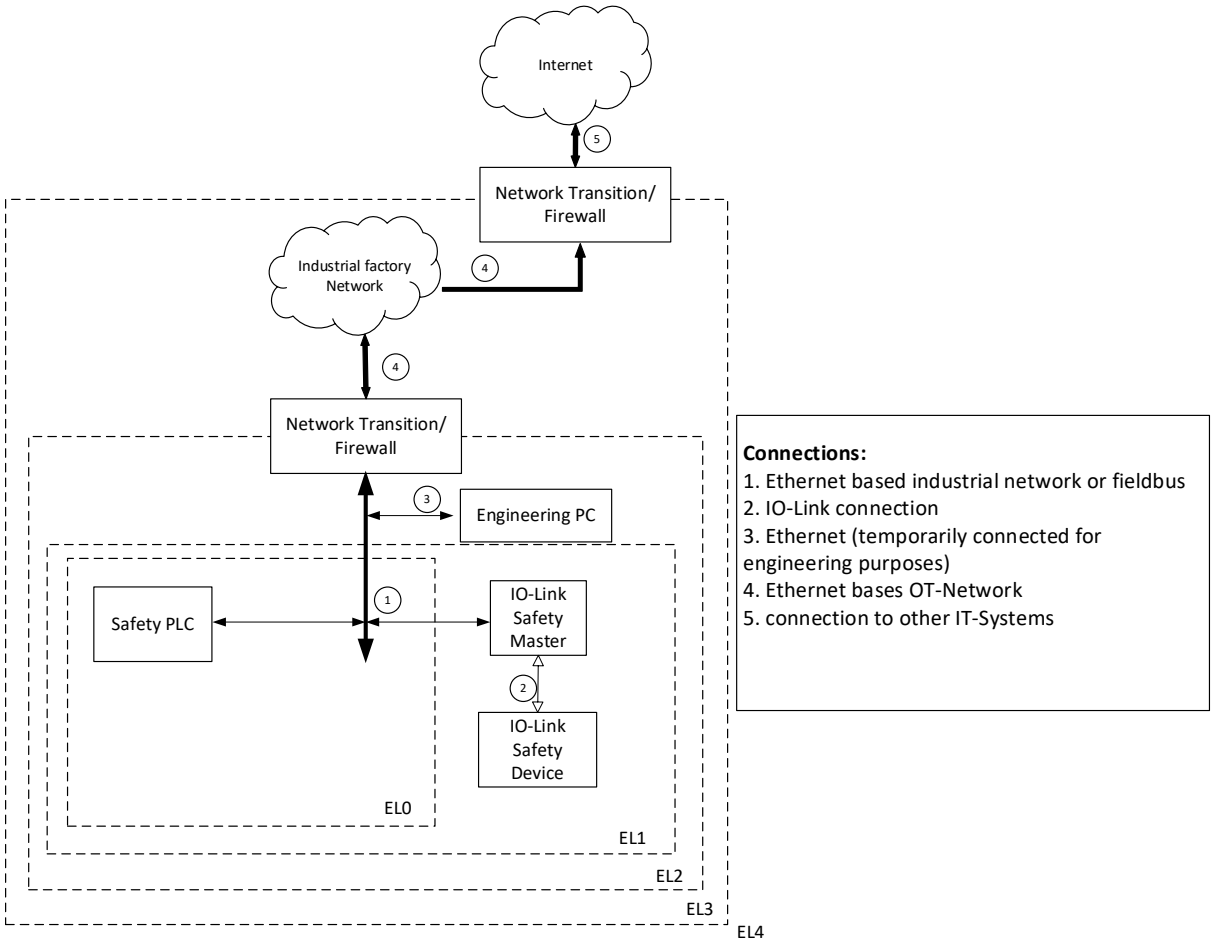

Abbildung 1: Datenfluss gemäß DIN EN50742

GERÄTE MIT SERIELLEM DIAGNOSEBUS (SD-BUS)

SYSTEMCHARAKTERISTIK DES SD-BUS

- Proprietärer, serieller Diagnosebus von Schmersal
- Reihenschaltung mehrerer Sicherheitssensoren (typisch bis zu 31 Devices)
- Übertragung von Status- und Diagnosedaten, keine sicherheitsgerichteten Funktionsdaten
- Anbindung an ein SD-Gateway, das die Daten in Feldbus- oder Ethernet-basierte Systeme überführt

Der SD-Bus selbst ist kein Netzwerk, sondern eine lokale serielle Verbindung.

PROTOKOLLSEITIGE SECURITY-EIGENSCHAFTEN DES SD-BUS

Der SD-Bus bietet keine integrierten Cybersecurity-Mechanismen:

- keine Verschlüsselung
- keine Authentifizierung
- keine Zugriffskontrolle
- lediglich einfache Integritätsprüfungen (z. B. CRC)
- keine Benutzer- oder Rollenmodelle

In dieser Hinsicht ist der SD-Bus vergleichbar mit IO-Link, jedoch funktional erweitert um eine zentrale Gateway-Anbindung.

SCHUTZZIELE UND RISIKOBEWERTUNG (ANALOG ZU IO-LINK)

Schutzziel	Risikobewertung	Begründung
Verfügbarkeit	hoch	Unterbrechung der seriellen Busverbindung stört die gesamte Diagnosekette
Integrität	hoch	Manipulierte Diagnosedaten können Fehlentscheidungen verursachen
Vertraulichkeit	niedrig–mittel	Offenlegung von Zustands-/Diagnosedaten bei physischem Zugriff
Authentifizierung / Zugriffskontrolle	nicht zutreffend	Keine protokollseitigen Mechanismen

BEDROHUNGSMODELL FÜR SD-BUS-GERÄTE

Physische Bedrohungen

- Manipulation oder Unterbrechung des SD-Bus
- Einschleusen eines manipulierten Geräts
- Abgriff von Diagnosedaten
- Sniffing oder Datenmanipulation mit Spezialhardware

Systemische Zusatzrisiken durch SD-Gateway

Im Gegensatz zu IO-Link entsteht ein erweitertes Risiko durch:

- Übergang SD-Bus → Feldbus / Ethernet
- Konfigurations- und Diagnosezugriffe auf das Gateway
- mögliche Remote-Zugriffe auf die Diagnoseebene

Der kritische Angriffspunkt ist nicht der SD-Bus selbst, sondern das SD-Gateway.

HANDLUNGSEMPFEHLUNGEN FÜR SD-BUS-GERÄTE

Physischer Schutz

- Schutz aller SD-Bus-Leitungen und angeschlossenen Devices
- Absicherung gegen unbefugtes Abstecken oder Einschleifen

Zonierung und Architektur

- Betrieb des SD-Bus innerhalb einer klar definierten Sicherheitszone
- Trennung von Diagnose- und Produktionsnetzwerken

Absicherung des SD-Gateways

- Zugriffskontrollen auf Konfigurationsschnittstellen
- Sichere Netzwerkintegration (Segmentierung, Firewalls)
- Protokollierung und regelmäßige Auswertung sicherheitsrelevanter Ereignisse

Bewertung nach MVO

Die nachfolgende schematische Darstellung zeigt, wie das Gerät nach der DIN EN 50742 im System eingebunden werden sollte, um den Schutz vor Korrumpierung zu gewährleisten:

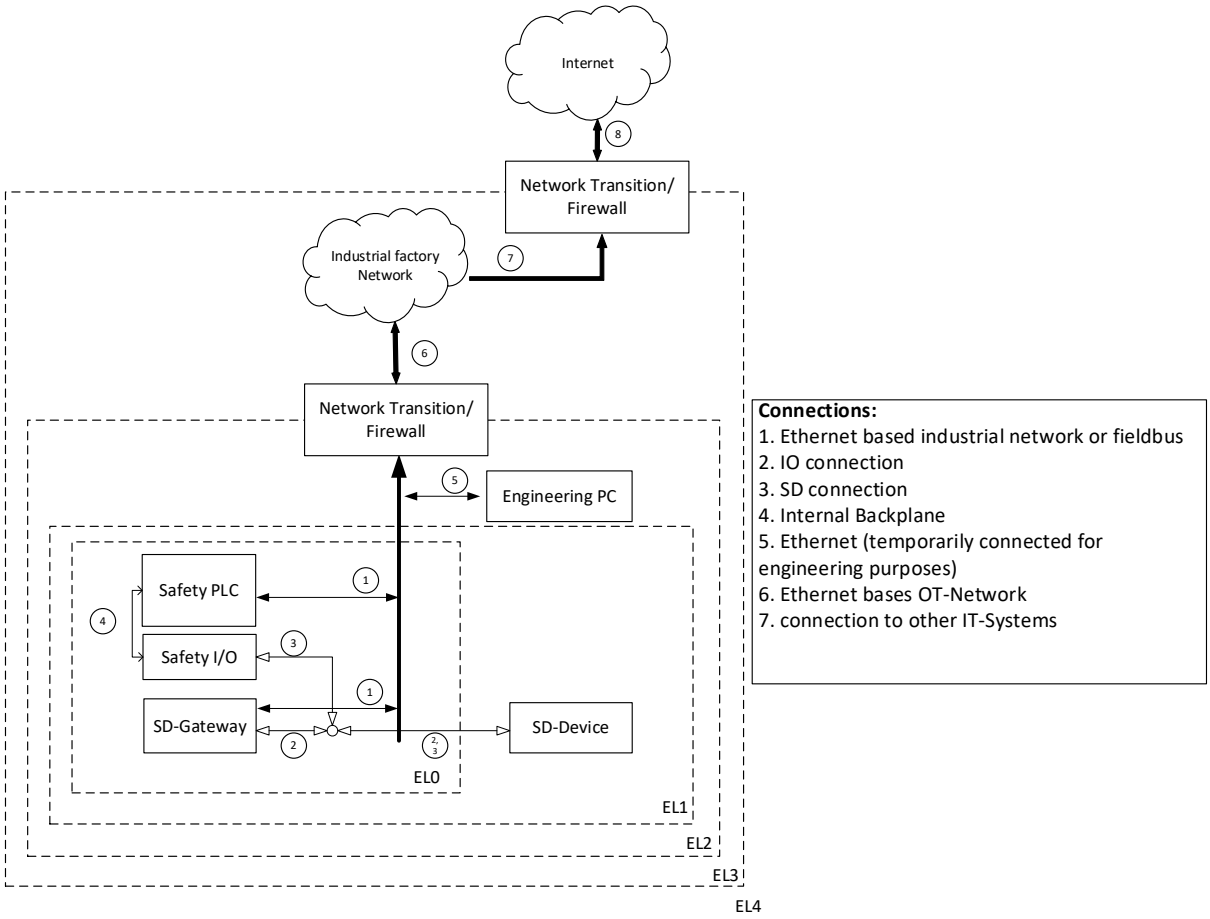

Abbildung 2: Datenfluss gemäß DIN EN50742

GERÄTE MIT AS-SCHNITTSTELLE (AS-I)

SYSTEMCHARAKTERISTIK DER AS-INTERFACE SCHNITTSTELLE

- Zweidraht-Leitung für:
  - Energieversorgung und
  - Datenkommunikation
- Freie Topologie möglich (Linie, Stern, Baumstruktur)
- Übertragung von Status- und Diagnosedaten, sicherheitsgerichtete Funktionsdaten
- Anbindung an ein AS-i Master/Gateway, das die Daten in Feldbus- oder Ethernet-basierte Systeme überführt

Die AS-Schnittstelle selbst ist kein Netzwerk, sondern eine lokale serielle Verbindung.

PROTOKOLLSEITIGE SECURITY-EIGENSCHAFTEN DER AS-I SCHNITTSTELLE

Die AS-Schnittstelle bietet keine integrierten Cybersecurity-Mechanismen:

- keine Verschlüsselung
- keine Authentifizierung
- keine Zugriffskontrolle
- keine Benutzer- oder Rollenmodelle

SCHUTZZIELE UND RISIKOBEWERTUNG

Schutzziel	Risikobewertung	Begründung
Verfügbarkeit	hoch	Unterbrechung der seriellen Busverbindung stört die gesamte Datenübertragung
Integrität	hoch	Manipulierte Daten können Fehlfunktionen verursachen
Vertraulichkeit	niedrig	Offenlegung von Zustands-/Diagnosedaten bei physischem Zugriff
Authentifizierung / Zugriffskontrolle	nicht zutreffend	Keine protokollseitigen Mechanismen

BEDROHUNGSMODELL FÜR AS-I GERÄTE

Physische Bedrohungen

- Manipulation oder Unterbrechung der AS-i Schnittstelle
- Abgriff von Diagnosedaten

Systemische Zusatzrisiken durch AS-Interface

- Übergang AS-i Feldbus / Ethernet
- Konfigurations- und Diagnosezugriffe auf das AS-i Gateway
- mögliche Remote-Zugriffe auf die Funktions- und Diagnoseebene

Der kritische Angriffspunkt ist nicht AS-i selbst, sondern das AS-i Gateway.

HANDLUNGSEMPFEHLUNGEN FÜR AS-I GERÄTE

Physischer Schutz

- Schutz aller AS-i Leitungen und angeschlossenen Devices
- Absicherung gegen unbefugtes Abstecken oder Einschleifen

Zonierung und Architektur

- Betrieb des AS-i Interface innerhalb einer klar definierten Sicherheitszone
- Trennung von Diagnose- und Produktionsnetzwerken

Absicherung des AS-i Gateways

- Verwendung von AS-i Gateways mit ausgewiesenen Security Maßnahmen
- Zugriffskontrollen auf Konfigurationsschnittstellen
- Sichere Netzwerkintegration (Segmentierung, Firewalls)
- Protokollierung und regelmäßige Auswertung sicherheitsrelevanter Ereignisse

Bewertung nach MVO

Die nachfolgende schematische Darstellung zeigt, wie das Gerät nach der DIN EN 50742 im System eingebunden werden sollte, um den Schutz vor Korrumpierung zu gewährleisten:

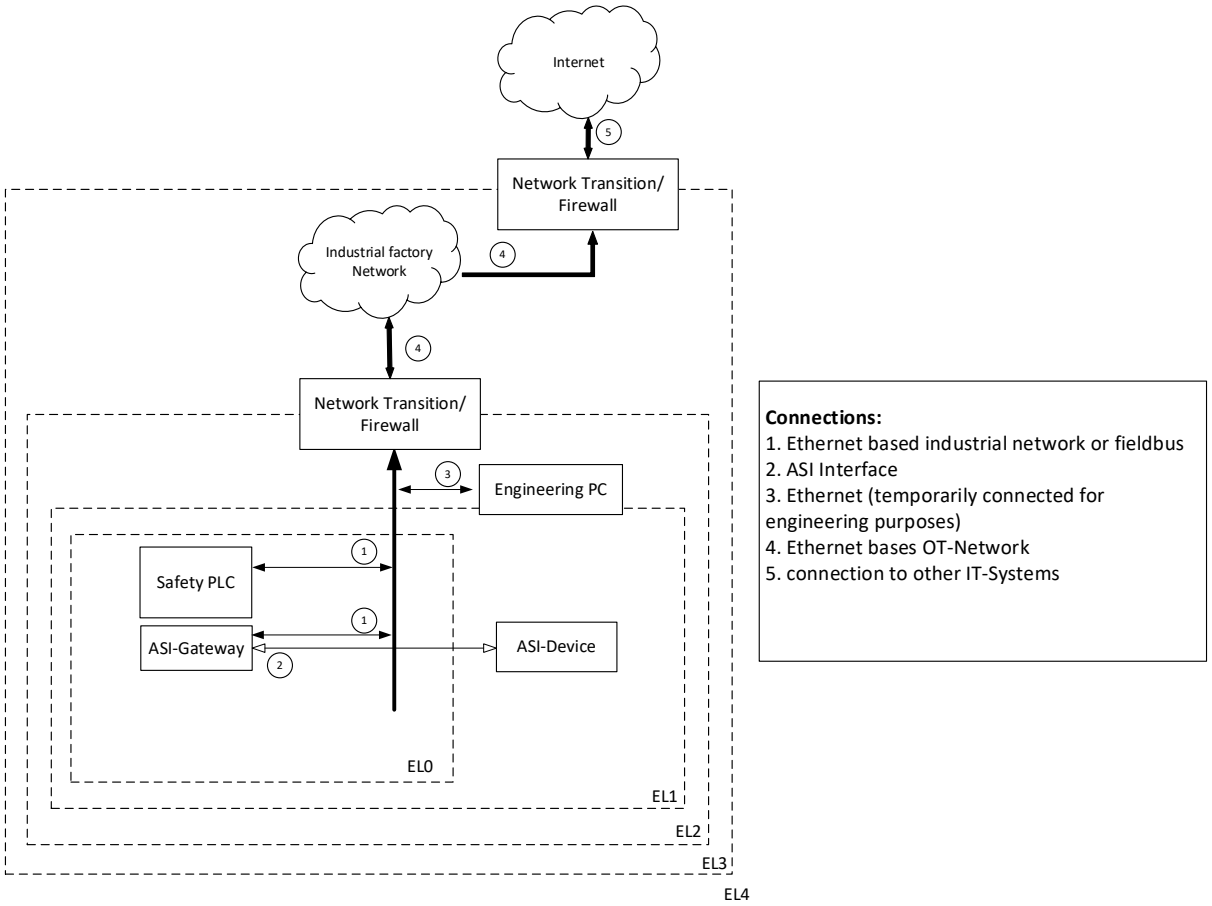

Abbildung 3: Datenfluss gemäß DIN EN50742

I/O-DEVICES

SYSTEMCHARAKTERISTIK DER I/O-SCHNITTSTELLE

- Digitale Sicherheits-Eingänge und Ausgänge (0V, 24V)
- Konventioneller digitaler Diagnoseausgang (0V, 24V)
- Keine klassische Buskommunikation
- Reihenschaltung der Sicherheitsfunktion möglich

Die I/O-Schnittstelle selbst ist kein Netzwerk, sondern eine lokale digitale Parallelverbindung.

SECURITY-EIGENSCHAFTEN DER I/O-VERBINDUNG

Die I/O-Schnittstelle bietet keine integrierten Cybersecurity-Mechanismen:

- keine Verschlüsselung
- keine Authentifizierung
- keine Zugriffskontrolle
- keine Benutzer- oder Rollenmodelle

SCHUTZZIELE UND RISIKOBEWERTUNG

Schutzziel	Risikobewertung	Begründung
Verfügbarkeit	hoch	Unterbrechung der I/O Kommunikation stört die gesamte Diagnosekette
Integrität	hoch	Manipulierte I/O Signale können Fehlfunktionen verursachen
Vertraulichkeit	niedrig	Offenlegung von Zustands-/Diagnosedaten bei physischem Zugriff
Authentifizierung / Zugriffskontrolle	nicht zutreffend	Keine Mechanismen umsetzbar

BEDROHUNGSMODELL FÜR I/O-GERÄTE

Physische Bedrohungen

- Manipulation oder Unterbrechung der I/O-Verbindung

Der kritische Angriffspunkt ist nicht die I/O-Parallelverbindung selbst, sondern die verbundene Auswerteeinheit oder Steuerung.

HANDLUNGSEMPFEHLUNGEN FÜR I/O-GERÄTE

Physischer Schutz

- Schutz aller I/O-Leitungen und angeschlossenen Devices
- Absicherung gegen unbefugtes Abstecken oder Einschleifen

Zonierung und Architektur

- Betrieb des I/O-Interface innerhalb einer klar definierten Sicherheitszone
- Trennung von Diagnose- und Produktionsnetzwerken

Absicherung der Auswerteeinheit

- Verwendung von einer Auswerteeinheit mit ausgewiesenen Security Maßnahmen
- Zugriffskontrollen auf Konfigurationsschnittstelle
- Sichere Netzwerkintegration (Segmentierung, Firewalls)
- Protokollierung und regelmäßige Auswertung sicherheitsrelevanter Ereignisse

Bewertung nach MVO

Die nachfolgende schematische Darstellung zeigt, wie das Gerät nach der DIN EN50742 im System eingebunden werden sollte, um den Schutz vor Korrumpierung zu gewährleisten:

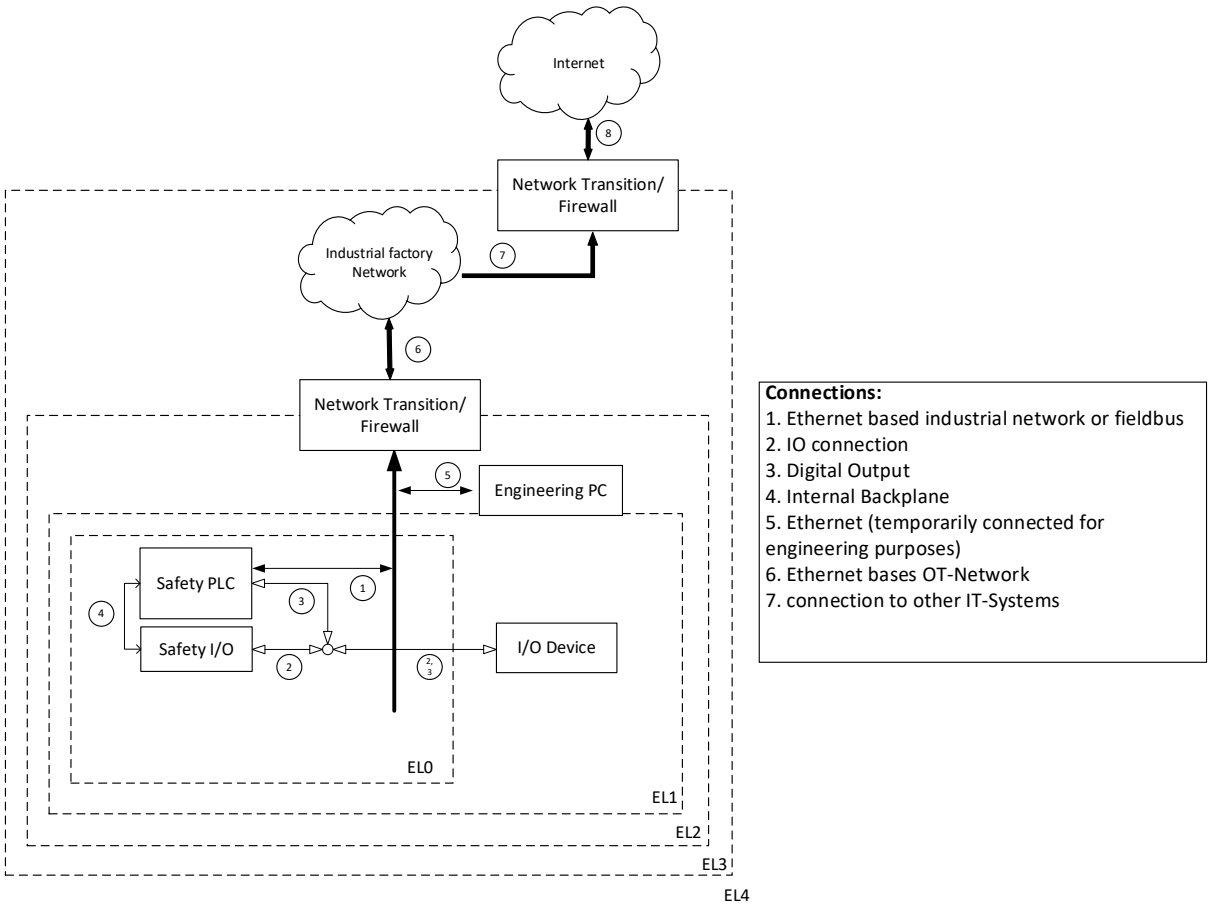

Abbildung 4: Datenfluss gemäß DIN EN50742

RFID

Die RFID-Übertragung basiert auf einem nicht öffentlichen und proprietären Datenprotokoll. Für einen ausreichenden Manipulationsschutz gemäß DIN EN ISO 14119 sind Geräte mit individueller Kodierung einzusetzen. (s. Typencode I2 / I1).

DIE SCHMERSAL GRUPPE
SICHERHEIT FÜR MENSCH UND MASCHINE

Die eigentümergeführte Schmersal Gruppe gehört im anspruchsvollen Aufgabenfeld der funktionalen Maschinensicherheit zu den internationalen Markt- und Kompetenzführern. Das 1945 gegründete Unternehmen beschäftigt rund 2.000 Mitarbeiterinnen und Mitarbeiter und ist mit sieben Produktionsstandorten auf drei Kontinenten sowie mit eigenen Gesellschaften und Vertriebspartnern in mehr als 60 Nationen präsent.

Zu den Kunden der Schmersal Gruppe gehören die Global Player des Maschinen- und Anlagenbaus sowie Anwender der Maschinen. Sie profitieren vom umfassenden Know-how des Unternehmens als System- und Lösungsanbieter für Maschinensicherheit. Darüber hinaus verfügt Schmersal über besondere Branchenkompetenz in verschiedenen Anwendungsfeldern; dazu gehören u. a. die Intralogistik, die Nahrungsmittelproduktion, die Verpackungstechnik, der Werkzeugmaschinenbau, die Aufzugtechnik, die Schwerindustrie sowie der Automobilsektor.

Zum Angebotsportfolio der Schmersal Gruppe trägt wesentlich der Geschäftsbereich tec.nicum mit seinem umfangreichen Dienstleistungsprogramm bei: Zertifizierte Functional Safety Engineers beraten Maschinenhersteller und -betreiber in allen Fragen der Maschinen- und Arbeitssicherheit – und das produkt- und herstellerneutral. Darüber hinaus planen und realisieren sie rund um den Globus komplexe Sicherheitslösungen in enger Zusammenarbeit mit den Auftraggebern.

SAFETY PRODUCTS

- Sicherheitsschalter und -sensoren, Sicherheitszuhaltungen
- Sicherheitssteuerungen und -relaisbausteine, Sicherheitsbussysteme
- Optoelektronische und taktile Sicherheitseinrichtungen
- Automatisierungstechnik: Positionsschalter, Näherungsschalter

SAFETY SYSTEMS

- Komplettlösungen für die Absicherung von Gefahrenbereichen
- Individuelle Parametrierung und Programmierung von Sicherheitssteuerungen
- Maßgeschneiderte Sicherheitstechnik – ob Einzelmaschine oder komplexe Fertigungsstraße
- Branchengerechte Sicherheitslösungen

SAFETY SERVICES

- tec.nicum academy – Schulungen und Seminare
- tec.nicum consulting – Beratungsdienstleistungen
- tec.nicum engineering – Konzeption und technische Planung
- tec.nicum integration – Ausführung und Montage
- tec.nicum digitalisation – Softwarelösungen und neue digitale Technologien
- tec.nicum oursourcing – Komplettlösungen

SCHMERSAL
THE DNA OF SAFETY

www.schmersal.com