FUNKTIONALE SAFETY-LÖSUNGEN

Sicherheitsprotokolle in drahtlosen Netzwerken

Vergleich der industriellen Safety-Protokolle und deren Leistungsstärke in drahtlosen Netzwerken

Vergleich der industriellen Safety-Protokolle und deren Leistungsstärke in drahtlosen Netzwerken

EINLEITUNG

ENTKOPPLUNG VON SICHERHEITSFUNKTIONEN

Jahrzehntelang waren die Sicherheitsfunktionen in den Systemen zur Fabrikautomatisierung fest verkabelt. Spezielle Kabel zur Übertragung von Sicherheitssignalen hatten sich in der Praxis bewährt und ermöglichten deterministische Reaktionen. In den vergangenen zehn bis fünfzehn Jahren haben Feldbustechnologien ihren Weg in die Automatisierungssysteme gefunden. Sie erlauben eine größere Flexibilität bei der Entwicklung von Maschinen und Anwendungen. Gleichzeitig wurden auch die Sicherheitssignale sukzessive in die konventionelle Feldbusinfrastruktur integriert. Auch wenn sie weiter über feste Netzwerkkabel übertragen werden, ermöglichte die neue Freiheit der Kommunikation über Feldbusse insgesamt eine wesentlich größere Flexibilität bei der Anwendung von Sicherheitsfunktionen. Genau wie die Geräte der Fabrikautomatisierung waren die Sicherheitsfunktionen an den Fabrikboden gebunden. Die gesamte Konzeption der sicheren Datenkommunikation über Feldbusnetzwerke erfolgte unter der Annahme robuster, zuverlässiger und fester Netzwerke.

Als sich die Räder der Automatisierung buchstäblich schneller zu drehen begannen, wurden auch die Komponenten der Fabrikautomatisierung immer agiler. In Lagern und Fabrikhallen kommt eine wachsende Armada mobiler Maschinen zum Einsatz. Das Zeitalter der mobilen Roboter in der Fabrikautomatisierung bringt neue Anforderungen an die sichere Datenkommunikation mit sich. Es mussten neue Methoden gefunden werden, um die Sicherheitsfunktionen von den kabelgebundenen Netzwerken zu entkoppeln und die Kommunikation mit einer zentralen Steuereinheit sowie untereinander in einer sich ständig bewegenden Umgebung zu ermöglichen. Daher ist die Sicherheit über drahtlose Technologien der entscheidende Faktor für die neue Freiheit der mobilen Maschinen.

Die am weitesten verbreitete und bekannteste Technologie für drahtlose Kommunikation ist das Wireless LAN (WLAN oder Wi-Fi), das im Standard IEEE802.11 beschrieben ist. Mit regelmäßigen Updates wird der zunehmenden Anzahl von Netzwerkgeräten, der Datenlatenz, den Roaming-Verzögerungen und dem Datendurchsatz in diesen Netzwerken Rechnung getragen. Daran lässt sich

INHALT

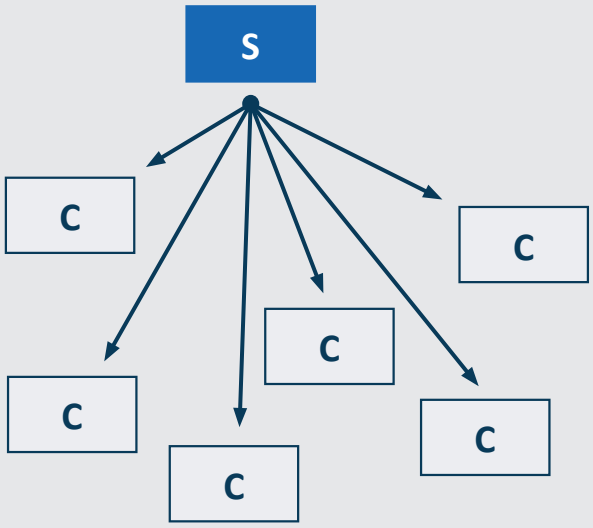

Abbildung 1: Kommunikationsbeziehung zwischen einzelnem Server und mehreren Clients

erkennen, wie die ursprünglich viel langsameren drahtlosen Technologien zu den bewährten kabelgebundenen Netzwerktechnologien mit hoher Bandbreite aufzuschließen versuchen.

All diese Fortschritte in der drahtlosen Kommunikation können jedoch schnell wieder zunichte gemacht werden, wenn ungeeignete Übertragungsprotokolle – sichere und unsichere – über das drahtlose Medium eingesetzt werden.
Daher liegt das Hauptaugenmerk des vorliegenden Whitepapers auf der Nutzbarkeit verschiedener Standard-Sicherheitsprotokolle in einer drahtlosen Umgebung.

SZENARIO FÜR DRAHTLOSE ANWENDUNGEN

In einem typischen Szenario kommunizieren mehrere Clients C, bei denen es sich um mobile Maschinen handeln kann, über große Entfernungen mit einer zentralen Steuereinheit oder, allgemein ausgedrückt, einem Server S (siehe Abbildung 1).

Durch den Einsatz mobiler Maschinen in Fabriken und Lagern entstehen zusätzliche Gefahrenquellen in der Arbeitsumgebung. Daher ist die Nutzung von Sicherheitsfunktionen unvermeidlich. So muss etwa ein Sicherheits-Not-Stopp-Signal von einem zentralen Server an bestimmte Clients in mobilen Maschinen gesendet werden. Sich schnell bewegende mobile Maschinen erfordern hohe Datenraten, geringe Latenzen und schnelles Roaming. Daher liegt der Schwerpunkt in diesem Whitepaper auf WLAN-Netzwerken (802.11), die diese Anforderungen besser erfüllen als andere drahtlose Technologien wie Bluetooth.

Trotz der kontinuierlichen technischen Fortschritte bleiben die grundlegenden Probleme von Funknetzwerken bestehen. Die Nutzung der Luft als „gemeinsames Medium“, die Störempfindlichkeit und die Anfälligkeit für Datenstaus wirken sich nachteilig auf die Kommunikation aus. Daraus ergeben sich höhere Anforderungen an die eingesetzten Übertragungsprotokolle, insbesondere an das Sicherheitsprotokoll. Nachfolgend werden daher zunächst die wichtigsten Eigenschaften bekannter Sicherheitsprotokolle dargelegt.

EIGENSCHAFTEN VON SICHERHEITSPROTOKOLLEN

Die in der IT-Welt genutzten Protokolle unterscheiden sich in den Anwendungsbereichen, für die sie ursprünglich bestimmt waren. Ein Protokoll zur Übertragung von Video-Streams muss andere Eigenschaften aufweisen als ein Protokoll zur Steuerung eines Roboters in der Produktion. Im vorliegenden Whitepaper befassen wir uns allerdings nur mit Protokollen für den Bereich der Sicherheitsanwendungen. Diese Protokolle ähneln sich zwar, unterscheiden sich aber erheblich in ihrer Anwendbarkeit im drahtlosen Bereich, für den sie ursprünglich nicht vorgesehen waren. Wie alle Protokolle sind Sicherheitsprotokolle hierarchisch

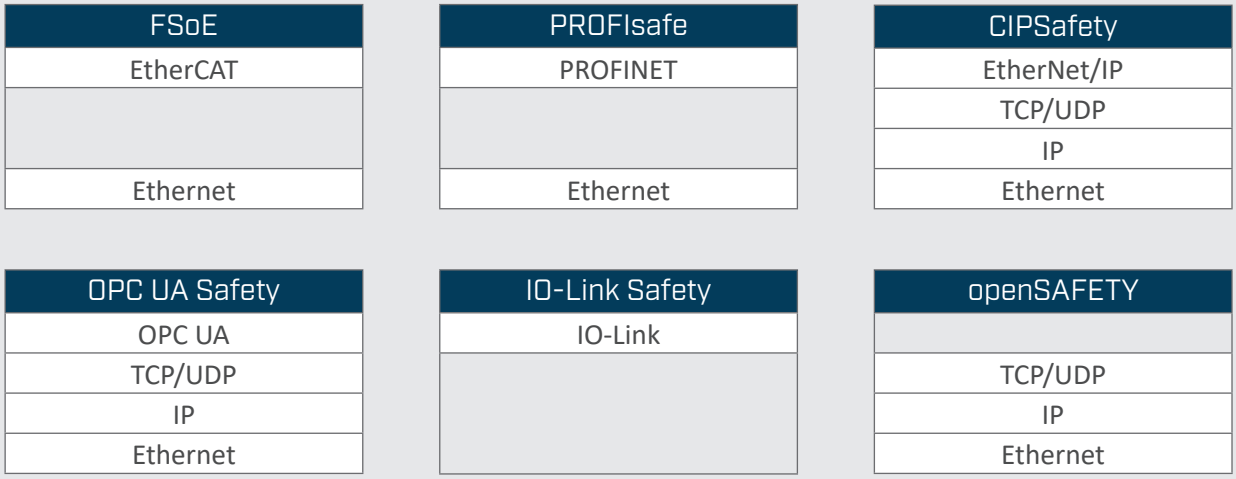

Abbildung 2: Stack an Schichten ausgewählter Sicherheitsprotokolle

strukturiert (Abb. 2). Alle Sicherheitsprotokolle weisen jeweils eine unterschiedliche Anzahl und Komplexität von Schichten auf. Bestimmte Zwischenschichten (z. B. die Kapselungsschicht von EtherNet/IP) werden in einigen Protokollen weggelassen.

Die jeweiligen Schichten erfüllen unterschiedliche Aufgaben. Die oberste Schicht stellt die Sicherheitsschicht dar. Die darunter liegenden Schichten bilden das Übertragungsprotokoll über den sogenannten „schwarzen Kanal". Zu den Aufgaben der Schichten zählen u. a. die Überwachung des Übertragungsvorgangs und der Verbindung oder die Weiterleitung von Paketen. Mit jeder weiteren Schicht nehmen jedoch auch die Paketgröße und damit das Datenvolumen zu.

Die gängigsten Sicherheitsprotokolle (in Abbildung 2 aufgelistet) beruhen auf unterschiedlichen Kommunikationsmodellen. In einem Client-Server-Modell erfolgt die Kommunikation über eine Abfolge von Anfrage und Antwort. Die Daten werden in beide Richtungen mit der gleichen Frequenz gesendet.

Bei einem Erzeuger-Verbraucher-Modell werden die Daten ohne vorherige Anfrage übermittelt. Im Prinzip erfolgt die Übertragung nur in einer Richtung. Das entspricht einem Datenstrom.

Bei den meisten Sicherheitsprotokollen befinden sich die Kommunikationsteilnehmer in einer Master-Slave-Beziehung. Die Verbindung wird durch einen zentralen Master hergestellt, über den der Datenaustausch erfolgt. Die direkte Kommunikation zwischen den Slaves wird nicht unterstützt. Dadurch sind dem Erzeuger-Verbraucher-Modell Grenzen gesetzt. Die von einem Slave erzeugten Daten müssen von einem anderen Slave über den Master verbraucht werden.

Bei Sicherheitsanwendungen ist es normalerweise wichtiger, dass die neuesten Daten empfangen werden, als dass alle Daten empfangen werden. Es würde beispielsweise keinen Sinn machen, den verlorenen Positionswert eines Positionsgebers zu wiederholen, wenn dieser bereits einen neuen Positionswert gesendet hat. Genauso wäre es wenig sinnvoll, ein Not-Stopp-Signal zu wiederholen, wenn es ohnehin regelmäßig gesendet wird. Aus der Sicht des Übertragungsprotokolls können Bestätigungen und Wiederholungen von Meldungen dann wegfallen. Ein weiterer Vorteil des Erzeuger-Verbraucher-Modells ist die unbegrenzte

Anzahl der Verbraucher. Ein Erzeuger kann zahlreiche Verbraucher haben. Dies wird bei einigen Protokollen sogar insofern unterstützt, als der Erzeuger die Daten nur einmal senden muss, sie aber von mehreren Verbrauchern verarbeitet werden können.

Darüber hinaus gibt es verschiedene Methoden der Datenübertragung:

Verbindungen
Bei einigen Protokollen werden für die verschiedenen Übertragungsrichtungen separate Verbindungen verwendet. Damit können zwar beispielsweise mehrere Verbraucher die gleichen erzeugten Daten empfangen, doch bei bidirektionaler Übertragung der Daten zwischen den Stationen müssen zwei einzelne Verbindungen aufrechterhalten werden.

Übertragungsarten
Bei einer periodischen Übertragung spielt es keine Rolle, ob sich die Daten ändern oder nicht. Im Gegensatz dazu werden bei Change-of-State-Verbindungen die Daten nur dann übertragen, wenn sie sich geändert haben. Da jedoch aus Sicherheitsgründen regelmäßig ein „Lebenszeichen“ der Verbindung gesendet werden muss, ist neben der Übertragung der Statusänderung auch eine periodische Übertragung erforderlich. In solch einem Fall bestimmt in aller Regel die Anwendung, wie oft dieses Lebenszeichen gesendet werden soll, um eine stabile Verbindung zu gewährleisten.

Datenpriorität
Neben Prozessdaten werden mit Protokollen auch administrative Daten übertragen. Deren Übertragung ist im Allgemeinen nicht so zeitkritisch. Daher bieten einige Protokolle die Option, den Prozessdaten bei der Übertragung Vorrang einzuräumen. Das ist ein Beispiel für Quality of Service.

Die verschiedenen Eigenschaften bekannter Sicherheitsprotokolle werden in der nachstehenden Tabelle verglichen. Die Abkürzungen haben die folgende Bedeutung:

- **KM** (Kommunikationsmodell)
  Möglich ist hier eine Client-Server-Beziehung, die auf einer Anfrage-Antwort-Kommunikation basiert, oder eine Erzeuger-Verbraucher-Beziehung, bei der ein Verbraucher die Daten ohne vorherige Anfrage erhält.

- **SV** (Separate Verbindungen)
  Für die bidirektionale Übertragung von Nutzerdaten werden separate Verbindungen verwendet.

- **GD** (Gemeinsame Daten)
  Gemeinsame Nutzung der Nutzerdaten. Die Nutzerdaten werden nur einmal über das physische Medium gesendet, aber von mehreren Netzwerkteilnehmern empfangen und verarbeitet.

- **FS** (Flusssteuerung)
  Sie verhindert Datenverluste aufgrund von Pufferüberläufen. Mindestens eine der Schichten erfordert eine Bestätigung der über das Kommunikationsmedium gesendeten Frames.

- **EÜ** (Erneute Übertragung)
  In mindestens einer der Schichten werden unbestätigte oder verlorene Frames erneut übertragen.

- **QoS** (Quality of Service)
  In Form einer Priorisierung der Meldungen auf dem Kommunikationskanal.

- **PE** (Protokolleffizienz)
  Verhältnis der Framing-Daten (Header/Trailer) zu den eigentlichen Anwendungsdaten.

Protokoll	KM	SV	GD	FS	EÜ	QoS	PE
OPC UA Safety	Client-Server	✓	✗	✓	✓	✗	- -
CIP Safety	Erzeuger-Verbraucher 1:1 bis zu 1:15	✓	✓	✗	✓	✓	-
FSoE	Client-Server	✗	✗	✓	✗	✗	+
PROFIsafe	Client-Server	✗	✗	✓	✓	✓	+

Tabelle 1: Eigenschaften ausgewählter Sicherheitsprotokolle

✗ = nein, ✓ = ja, + = effizienter, - = weniger effizient, -- = deutlich weniger effizient

Schlussfolgerungen

Separate Verbindungen: OPC UA Safety und CIP Safety nutzen zwei unabhängige bidirektionale Verbindungen, wenn Nutzerdaten zwischen zwei Stationen in beide Richtungen übertragen werden. Daraus resultieren insgesamt vier Übertragungsmeldungen für den Austausch der Nutzerdaten in beide Richtungen. PROFIsafe und FSoE dagegen verwenden nur eine bidirektionale Verbindung für diese Art der Übertragung von Nutzerdaten. Somit werden für den Austausch der Nutzerdaten in beide Richtungen insgesamt nur zwei Meldungen benötigt.

Gemeinsame Daten: CIP Safety ist das einzige Protokoll, bei dem dieselben Daten per Multicasts gleichzeitig von mehreren Empfängern ausgewertet werden können. Die Anzahl der Empfänger ist allerdings auf maximal 15 begrenzt.

Flusssteuerung: Bei einer Anfrage-Antwort-Kommunikation stellt die Antwortmeldung die Bestätigung dar, dass die Anfrage empfangen wurde. Das Ausbleiben einer Antwort wird zeitlich überwacht. Bei einer Anfrage-Antwort-Kommunikation, die einer Flusssteuerung mit der Fenstergröße 1 entspricht, darf nur eine Anfragemeldung zur Bestätigung ausstehen.

Da CIP Safety auf dem Erzeuger-Verbraucher-Modell basiert, überwacht die Sicherheitsschicht die Verbindung, indem sie regelmäßig Bestätigungspakete in die entgegengesetzte Richtung zur Übertragung der Nutzerdaten sendet. Diese Bestätigungspakete werden jedoch nicht zur Flusssteuerung der Nutzerdatenpakete eingesetzt.

Erneute Übertragung: Die erneute Übertragung von Meldungen erfolgt nur bei Protokollen, die TCP/IP für die Übertragung von Management-Frames nutzen. Prozessdaten dagegen werden niemals erneut übertragen.
Die Protokolle OPC UA Safety und CIP Safety weisen viele Schichten auf, selbst bei der Übertragung von Prozessdaten. Eine davon ist die IP-Schicht, die die Weiterleitung von Prozessdaten über verschiedene Netzwerke ermöglicht, einschließlich Funknetzwerken. Ein Nachteil der zahlreichen Schichten besteht darin, dass das Verhältnis von Nutzerdaten zu administrativen Daten ungünstiger ist als bei anderen Protokollen.

SICHERHEITSPROTOKOLLE IN EINER DRAHTLOSEN UMGEBUNG

Nachfolgend werden einige typische Anwendungsszenarien mit unterschiedlichen Sicherheitsprotokollen vorgestellt. FSoE wird hier nicht behandelt, da die EtherCAT-Transportschicht für die drahtlose Übertragung ungeeignet ist. Die Beispiele sollen eine Vorstellung vom Datenvolumen und von den Unterschieden zwischen den verschiedenen Protokollen vermitteln. Daher wird von einer optimalen Umgebung ausgegangen. So werden beispielsweise die regelmäßig erfolgenden 802.11-Neuübertragungen ebenso vernachlässigt wie die nicht sicherheitsbezogene Kommunikation über die drahtlosen Medien. Es wird davon ausgegangen, dass die volle Bandbreite der Access Points für die Übertragung der Sicherheitsprozessdaten zur Verfügung steht und genutzt wird.

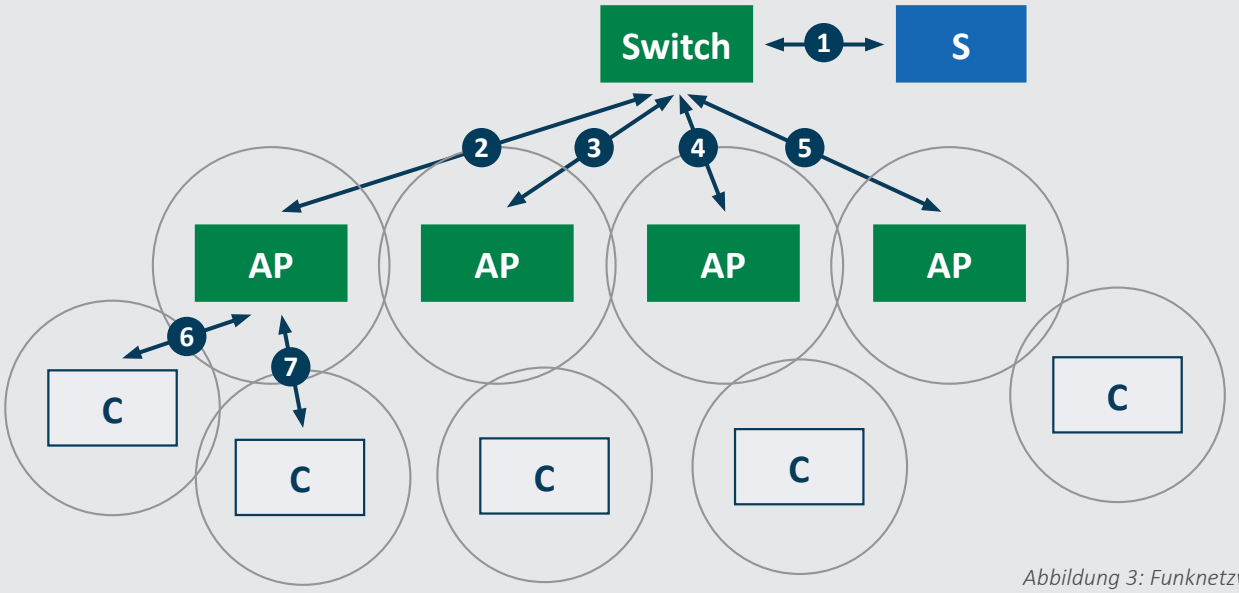

Abbildung 3: Funknetzwerk für unidirektionale Übertragung

Unidirektionale Übertragung von Sicherheitsdaten

Die Abbildung oben zeigt ein WLAN, bestehend aus Access Points (AP), Clients (C), einem Server (S) und einem Switch. Die APs überbrücken das drahtlose 802.11 und das kabelgebundene Ethernet. Sie sind über einen zentralen Switch mit dem Server verbunden (siehe Abbildung 3).

In diesem Beispiel wird ein Sicherheits-Not-Stopp-Signal vom Server (SPS) an die Clients übertragen. Aufgrund der Dringlichkeit des Not-Stopp-Signals werden diese Sicherheitsprozessdaten unidirektional mit einer hohen Datenrate übertragen, um schnelle, sichere Reaktionszeiten zu erreichen.

CIP Safety

Da CIP Safety nur höchstens 15 verbrauchende Clients bei einer Multicast-Sicherheitsverbindung unterstützt, gehen wir davon aus, dass alle CIP-Safety-Verbindungen Singlecast sind und somit jeder Client einen eigenen Kommunikationskanal zum Server verwenden soll. Bei **n** Clients werden n verbrauchende Singlecast-Sicherheitsverbindungen hergestellt. Infolgedessen werden **n** bidirektionale EtherNet/IP-Verbindungen und somit n UDP/IP-Verbindungen aufrechterhalten.

Bei **m** Access Points und einer gleichmäßigen Verteilung der Clients auf die APs überträgt der drahtlose Kommunikationskanal (6, 7) zwischen den Clients und einem einzelnen AP sequentiell **2 n/m** 802.11-Frames pro Prozessdatenzyklus.

Die kabelgebundenen Kanäle (2-5) zwischen einem AP und dem Switch übertragen jeweils **2 n/m** Ethernet-Frames. Das Kabel (1) zwischen dem Switch und dem Server überträgt **2 n** Ethernet-Frames.

Beispiel: n=100, n/m=20-> m=5-> ergibt 40 802.11-Frames pro Funkzelle und Zyklus. Bei einer Frame-Größe von 70 Bytes (die meisten davon Framing-Bytes) und einem Nettodurchsatz von 20 Mbit/s (Anybus Wireless Bridge von HMS [AWB3000]) ist eine Zykluszeit von etwa 1 ms erreichbar.

Die Bestätigungsmeldungen können mit einer geringeren Rate übertragen werden als die Nutzerdaten. In diesem Fall verringert sich die Datenmenge in einer Funkzelle entsprechend. **Die Zykluszeit kann sich theoretisch 0,6 ms annähern.**

Bislang nicht berücksichtigt wurden die zusätzlichen azyklischen Frames für die Herstellung der CIP-Safety-Verbindungen, die bei Verbindungsabbrüchen erforderlich sind.

PROFIsafe

PROFIsafe nutzt unabhängig von der Richtung der Prozessdatenübertragung bidirektionale Verbindungen. Das bedeutet, dass bei einem unidirektionalen Prozessdatenfluss die Hälfte der Meldungen der Anfrage-Antwort-Kommunikation leer (ohne Prozessdaten) gesendet wird. Bei n Clients werden **n** verbrauchende Singlecast-Sicherheitsverbindungen durch den Server (Master) hergestellt. Infolgedessen werden **n** bidirektionale PROFINET-Verbindungen und somit **n** Ethernet-Verbindungen aufrechterhalten.

Die Verteilung der Clients und des Datenvolumens auf die Funkzellen ist die gleiche wie im Beispiel für CIP Safety oben.

Beispiel: n=100, n/m=20-> m=5-> ergibt 40 802.11-Frames pro Funkzelle und Zyklus. Bei einer Frame-Größe von 33 Bytes (die meisten davon Framing-Bytes) und einem Nettodurchsatz von 20 Mbit/s (Anybus Wireless Bridge von HMS [AWB3000]) **ist eine theoretische Zykluszeit von etwa 0,5 ms erreichbar.**

Das Datenvolumen von PROFIsafe ist fast das gleiche wie das von CIP Safety. Der Nachteil von PROFIsafe, dass die Pakete mit der gleichen Zykluszeit in die entgegengesetzte Richtung zur Nutzerdatenübertragung gesendet werden, wird durch den Vorteil wettgemacht, dass PROFIsafe weniger Framing-Daten verwendet als CIP Safety.

OPC UA Safety

Genau wie PROFIsafe nutzt OPC UA Safety bidirektionale Meldungen für jede Datenverbindung, und zwar unabhängig von der Übertragungsrichtung der Anwendungsdaten. Das bedeutet, dass für die Übertragung eines sicherheitsbezogenen Nutzerdatenpakets zwei Meldungen erforderlich sind. Bei einer unidirektionalen Datenkommunikation sendet OPC UA Safety die Hälfte der Anfrage-Antwort-Meldungen ohne Prozessdaten, genau wie PROFIsafe. Allerdings ist der Overhead an Framing-Bytes höher als bei PROFIsafe.

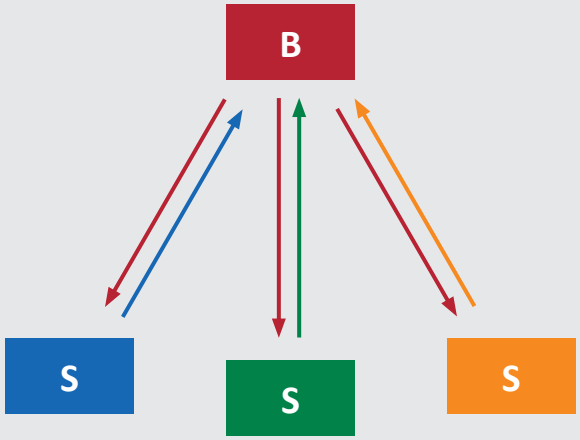

Abbildung 5: Datenkommunikation über Broker

Bidirektionale Übertragung von Sicherheitsdaten

In diesem Szenario sollen die Daten zwischen den Stationen (S) eines Funknetzwerkes über bidirektionale Verbindungen ausgetauscht werden. Die Daten sollen also von jeder Station zu jeder Station übertragen werden (siehe Abbildung 4).

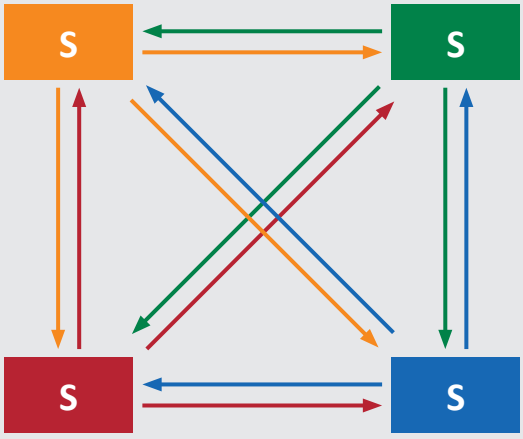

Abbildung 4: Vollständig vernetzte bidirektionale Datenübertragung

Das führt zu einem extrem hohen Datenvolumen. Mit einem zentralen Daten-„Broker“ lässt sich dieses Datenvolumen verringern (siehe Abbildung 5). Beim Broker-Konzept gibt es nur eine bidirektionale Verbindung zwischen jeder Station und dem Broker, wodurch sich die Gesamtzahl der notwendigen Verbindungen für die Übertragung der Nutzerdaten verringert.

Ein weiterer Vorteil dieser zentralen Instanz: Das Netzwerk kann zentral konfiguriert werden, und die Verbindung zu den Stationen kann durch eine zentrale Instanz (z. B. den Broker B selbst) hergestellt werden. Dadurch werden die Leistungsanforderungen an die Stationen S gesenkt.

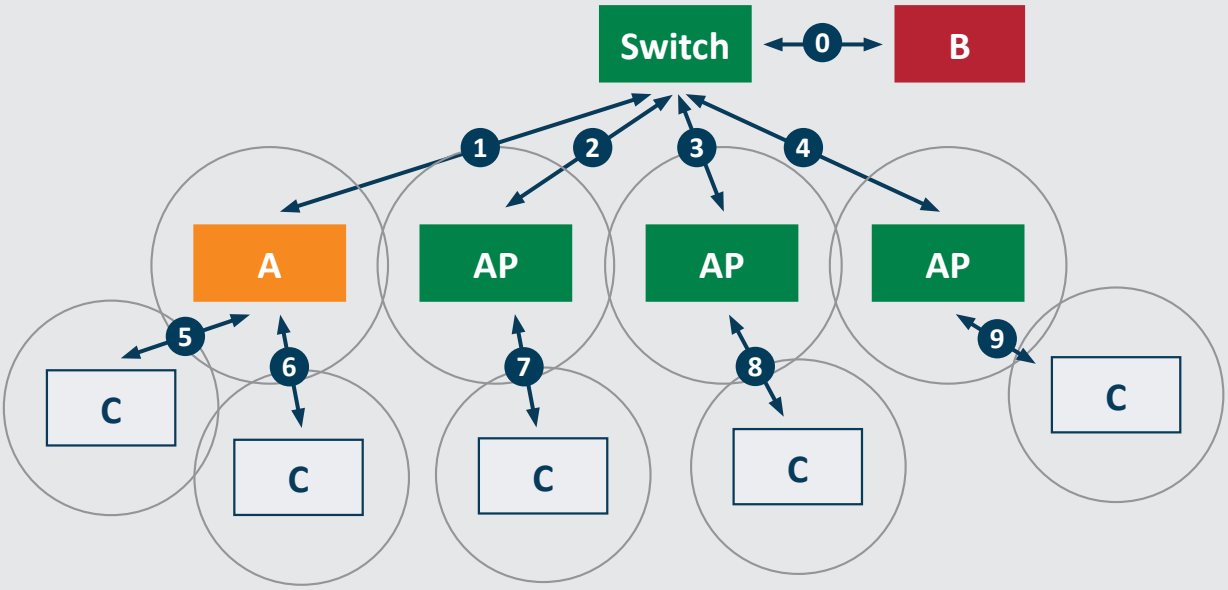

Abbildung 6: Funknetzwerk für bidirektionalen Datenaustausch

Abbildung 6 zeigt ein WLAN, bestehend aus Access Points (AP), Clients (C), einem Controller (B) und einem Switch. In diesem Beispiel sollen die Stationen sichere Anwendungsdaten untereinander austauschen, z. B. ihre 4-Byte-Positionswerte. Diese Art des Datenaustauschs kann durch einen zentralen Controller, einen Daten-„Broker“ B, realisiert werden. Dieser Broker sammelt alle Daten von den Clients und kann die gesammelten Daten wieder an alle relevanten Clients senden. In einem ersten Schritt sammelt der Broker B also die Positionswerte aller Clients C. Anschließend stellt er ein Prozessabbild mit allen gesammelten Positionswerten zusammen und sendet dieses an alle Clients. Abhängig von der maximal unterstützten Paketgröße des Sicherheitsprotokolls muss dieses Prozessabbild vom Broker in mehrere kleinere Sicherheits-Frames aufgeteilt werden.

CIP Safety

Wir gehen wieder davon aus, dass alle CIP-Safety-Verbindungen Singlecast sind. Bei n Clients werden n erzeugende Singlecast-Sicherheitsverbindungen für die Datenübertragung von den Clients zum Broker und n erzeugende Singlecast-Sicherheitsverbindungen für die Datenübertragung vom Broker zu den Clients hergestellt (Abbildung 7).

Infolgedessen werden **2n** bidirektionale EtherNet/IP-Verbindungen und somit **2n** UDP/IP-Verbindungen aufrechterhalten. Die Prozessdaten werden mit einer hohen Frame-Rate übertragen. Nachfolgend gehen wir davon aus, dass die Frames, die in entgegengesetzter Richtung zu den Prozessdaten übertragen werden, eine deutlich geringere Übertragungsrate aufweisen. Daher bleiben diese Frames hier unberücksichtigt.

Jeder Client sendet nur einen einzigen Frame an den Broker (das ist der positive Effekt des Broker-Konzeptes). Bei m Access Points und einer gleichmäßigen Verteilung der Clients auf die APs senden alle n/m Clients der Funkzelle A ihren IP-Frame an den Broker. Das erfordert n/m 802.11-Frames (5, 6).

Der Broker sammelt die Sicherheitsdaten aller Clients und sendet sie in einer Reihe von Sicherheitspaketen an alle Clients. Jeder AP empfängt dementsprechend c*n/m IP-Frames, wobei c die Anzahl der Frames ist, in die die Prozessabbilddaten des Brokers aufgeteilt sind. Diese werden in c*n/m 802.11-Frames konvertiert.

Folglich werden in einer Funkzelle (c+1)*n/m 802.11-Frames pro Prozessdatenzyklus übertragen.

Beispiel: n=100, n/m=20-> m=5, der Broker möchte ca. 400 Bytes senden-> diese Bytes werden wegen des Nutzerdaten-Limits von 250 Bytes pro Paket von CIP Safety mit zwei CIP-Safety-Frames gesendet-> c=2. Jedes CIP-Safety-Paket transportiert die Nutzerdaten und die ergänzenden Daten. Es ergeben sich 60 802.11-Frames pro Funkzelle und Zyklus. Bei einer Zahl von 400 vom Broker empfangenen Bytes plus Framing-Bytes (einschließlich ergänzender Daten), einer Frame-Größe von ca. 80 Bytes, die von den Clients zur Meldung ihrer sicheren Anwendungsdaten gesendet werden, und einem Nettodurchsatz von 20 Mbit/s (Anybus Wireless Bridge von HMS [AWB3000]) **ist eine theoretische Zykluszeit von etwa 8 ms erreichbar**. Das entspricht der Aktualisierungsrate des gesamten Sicherheitsprozessabbildes. Durch die aufgeteilte Übertragung der Prozessdaten verringert sich die effektive Zykluszeit der Pakete um etwa das Zweifache. Daher muss der Broker Sicherheitsverbindungen mit einer Zykluszeit von ca. 4 ms öffnen.

Die Bestätigungsmeldungen in entgegengesetzter Richtung zu den Prozessdaten wurden hier nicht berücksichtigt. Allerdings ist der Administrationsaufwand bei einer bidirektionalen Übertragung doppelt so hoch wie bei einer unidirektionalen Verbindung.

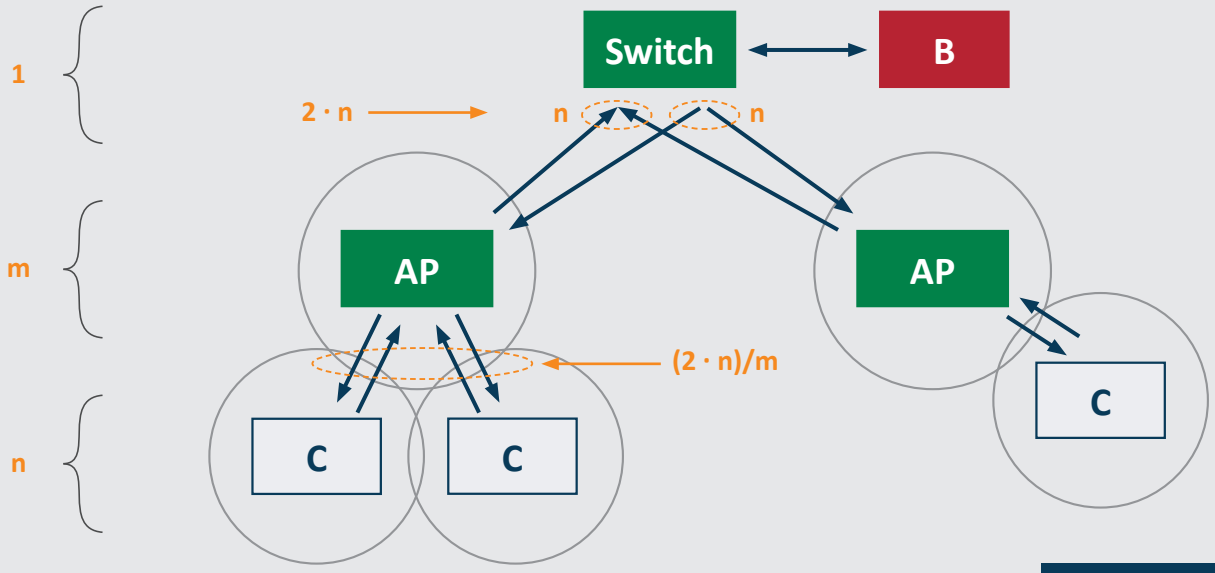

Abbildung 7: Anzahl der Meldungen bei bidirektionalem Datenaustausch für CIP Safety

PROFIsafe

PROFIsafe nutzt bidirektionale Verbindungen für die Übertragung von Prozessdaten. Bei n Clients werden n Singlecast-Sicherheitsverbindungen hergestellt. Infolgedessen werden **n** Ethernet-Verbindungen aufrechterhalten (siehe Abbildung 8). PROFIsafe unterstützt nur maximal 123 Bytes an Prozessdaten pro Frame. Der Aufteilungsfaktor ist größer als bei CIP Safety. Darüber hinaus müssen alle Frames bestätigt werden. Das führt zu einer deutlich höheren Anzahl von Frames pro Zelle für die Übertragung des Sicherheitsprozessdatenabbildes.

Beispiel: n=100, n/m=20-> m=5, der Broker möchte ca. 400 Bytes senden-> diese Bytes werden wegen des Nutzerdaten-Limits von 123 Bytes pro Paket von PROFIsafe mit vier PROFIsafe-Frames gesendet-> c=4. Wir gehen davon aus, dass die Clients ihre Positionswerte mit den Antwort-Frames der empfangenen Broker-Frames senden. Es ergeben sich 80 empfangene 802.11-Frames und 80 gesendete Antwort-Frames pro Funkzelle und Zyklus. Bei einer Zahl von 400 vom Broker empfangenen Bytes plus Framing-Bytes, einer Frame-Größe von ca. 30 Bytes, die von den Clients gesendet werden, und einem Nettodurchsatz von 20 Mbit/s (Anybus Wireless Bridge von HMS [AWB3000])

ist eine theoretische Zykluszeit von etwa 5 ms erreichbar. Das entspricht der Aktualisierungsrate des Sicherheitsprozessdatenabbildes. Durch die aufgeteilte Übertragung des Prozessdatenabbildes verringert sich die erforderliche Zykluszeit der Pakete um etwa das Vierfache. Daher muss der Broker Sicherheitsverbindungen mit einer Zykluszeit von ca. 1 ms öffnen.

Das Ergebnis ist besser als das von CIP Safety. Allerdings muss berücksichtigt werden, dass 802.11 aufgrund der höheren Zahl von PROFIsafe-Meldungen mehr Bestätigungs-Frames senden muss.

OPC UA Safety

Genau wie CIP Safety nutzt OPC UA Safety zwei bidirektionale Verbindungen, um Nutzerdaten in beide Richtungen zwischen zwei Knoten zu übertragen. Insgesamt sind in diesem Beispiel vier Meldungen an der Übertragung der Nutzerdaten beteiligt. Die beteiligten Meldungen müssen jedoch für jede Übertragungsrichtung eines Nutzerdatenpakets immer mit der gleichen Zykluszeit übertragen werden. CIP Safety hingegen erlaubt unterschiedliche Zykluszeiten für die an einem bidirektionalen Datenaustausch beteiligten Meldungen. Darüber hinaus ist der Overhead für Framing-Bytes bei OPC UA Safety höher als bei CIP Safety und PROFIsafe.

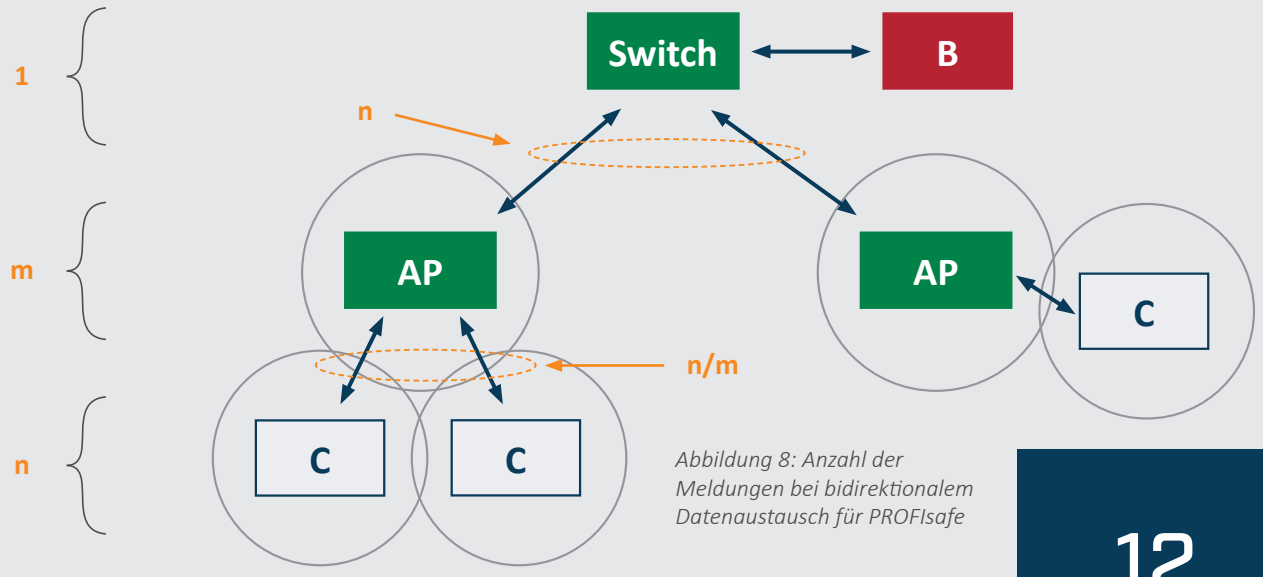

Abbildung 8: Anzahl der Meldungen bei bidirektionalem Datenaustausch für PROFIsafe

Fazit

Die hier vorgestellten Sicherheitsprotokolle haben alle ihre Vor- und Nachteile. Die Vorteile von CIP Safety liegen in der Gewichtung von Prozess- und Überwachungsdaten. Hinzu kommt die Routing-Fähigkeit der Prozessdaten aufgrund der Verwendung der standardmäßigen IP-Schicht. Zu den Nachteilen gehören die Verdoppelung der Nutzerdaten, die umfangreichen Framing-Informationen und die Verwaltung von zwei Verbindungen für die bidirektionale Datenübertragung. Die explizite Verbindungsverwaltung von CIP Safety führt außerdem zu mehr Datenverkehr beim Verbindungsaufbau, z. B. bei einem Verbindungsabbruch aufgrund einer gestörten Funkverbindung.

PROFIsafe hat einen geringeren Overhead an Framing-Informationen, erfordert aber die Übertragung von Daten in beide Richtungen mit der gleichen Frequenz. Zudem wird wegen der fehlenden IP-Adressierungsschicht kein Routing unterstützt.

Bei allen Protokollen können die Timeout-Parameter an die in der Regel höheren Latenzen angepasst werden, die durch das drahtlose Medium verursacht werden.

Um die maximale Leistung und Stabilität eines sicheren Funknetzwerkes zu erreichen, müssen verschiedene Parameter und architektonische Entscheidungen berücksichtigt werden. Wie oben gezeigt, werden die erreichbaren Kommunikationszykluszeiten je nach verwendetem Sicherheitsprotokoll auch von den Beziehungen der Anwendungsdaten beeinflusst.

Die Zykluszeiten der oben genannten Beispiele sind theoretischer Natur und sollen die allgemeinen Auswirkungen der Sicherheitsprotokolle selbst sowie der Richtungen der Datenkommunikation verdeutlichen. Im Grunde wird nicht die volle Funkbandbreite für den sicheren Datenaustausch genutzt. Zudem müssen erneute Übertragungen aufgrund von vorübergehend schlechten Funkverbindungen berücksichtigt werden.
In realen Funknetzwerken mit CIP Safety oder PROFIsafe werden typischerweise 10- bis 100-mal höhere Zykluszeiten als die theoretisch möglichen benötigt, um eine stabile Sicherheitsdatenverbindung zu erreichen.

Referenzen

[1] OPC UA Safety: Functional Safety Communication with OPC UA, Version 1, September 2022, https://opcfoundation.org/wp-content/uploads/2022/09/OPCF-OPCUA-Safety-EN.pdf

[2] Online-Referenz zu OPC UA, Teil 15: Sicherheit
https://reference.opcfoundation.org/Safety/docs/#5

[3] HMS, Whitepaper, Wireless technologies for industrial communication,
https://www.anybus.com/products/wireless-solutions/wireless-wp