funktionale sicherheit

powered by

Elektronik
Fachmedium für industrielle Anwender und Entwickler

Computer & Automation
Fachmedium der Automatisierungstechnik

Elektronik automotive
Fachmedium für professionelle Automobilelektronik

Safety und Wireless – (wie) geht das?

Der drahtlosen Kommunikation schlägt im Industrieumfeld nicht selten Skepsis entgegen – insbesondere wenn es um sicherheitsrelevante Anwendungen geht. Dabei lässt sich die Frage, ob sich drahtlose Übertragungstechniken auch für Safety eignen, heute eindeutig mit Ja beantworten.

Von Thomas Schildknecht

Hört man sich bei den Betreibern von Industrieanlagen um, so wird von ihnen der Einsatz von Funkstrecken zwar grundsätzlich gewünscht, gleichzeitig aber oft zurückhaltend beurteilt: Gewünscht, weil sich damit viele Installationsprobleme – vor allem bei bewegten oder schwer zugänglichen Anlagenteilen – einfach und kostengünstig lösen lassen; zurückhaltend beurteilt, weil Funkstrecken bezüglich ihrer Stabilität und Verfügbarkeit einer Kabelverbindung unterlegen sind.

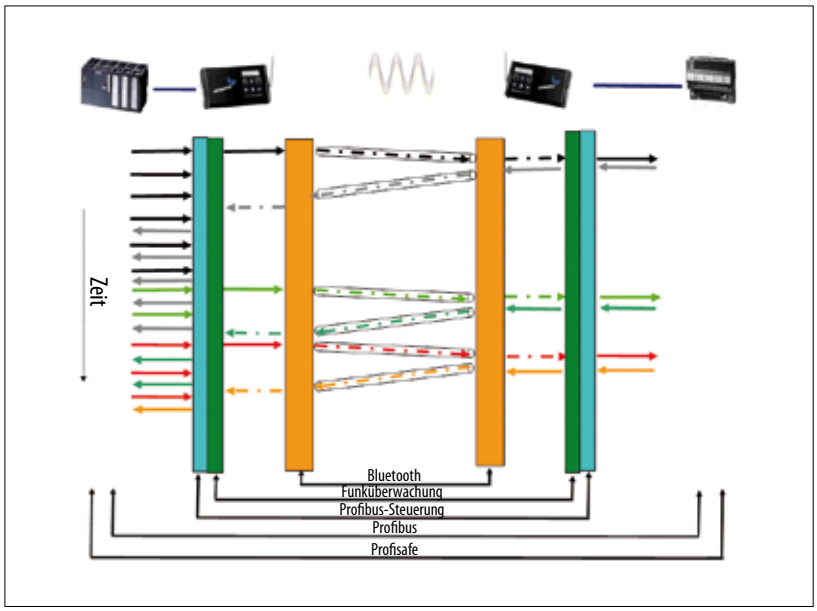

Bild 1. Funktionsblöcke und Kommunikationsablauf im Dataeagle-Funkmodul.

Zwar sind Störquellen für eine Funkstrecke in einer komplex aufgebauten Anlage grundsätzlich nicht völlig zu verhindern; vermeiden lässt sich jedoch der Einfluss solcher Störungen auf die Steuerung und damit auf die Anlagenverfügbarkeit. Dazu verhelfen im Wesentlichen zwei Maßnahmen:

- Die Projektierung der Funkstrecke – besonders die Wahl der Funktechnologie – muss anlagengerecht, das heißt unter Beachtung aller denkbaren Umfeldeinflüsse erfolgen.
- Die eingesetzten Funkmodule sollten über die „Intelligenz" verfügen, kurzfristige Funkstörungen rechtzeitig zu erkennen, zu interpretieren und deren Rückwirkung auf die Kommunikation zwischen Steuerung und Geräten weitgehend zu verhindern. Die Funkmodule sollen also eine intelligente Aufbereitungs- und Filterfunktion zwischen Steuerung, Funkstrecke und den nach der Funkstrecke angeordneten Kommunikationsteilnehmern wahrnehmen.

Die Technologie für eine derart abgesicherte Funkverbindung wurde bereits vor vielen Jahren zum Einsatz in Profibus-Netzen entwickelt und seither unter Einbeziehung der Anwender praxisorientiert optimiert. Die gerätetechnische Umsetzung in der sogenannten Dataeagle-Serie (DE) von Schildknecht erfolgt durch Hard- und Software, die als zwei zusätzliche Funktionsblöcke im Funkmodul implementiert werden. Diese Funktionsblöcke trennen die Funkstrecke rückwirkungsfrei von der Steuerung (Master) und den Geräten (Slaves), was zu einer hochverfügbaren und trotzdem schnellen Funkübertragung von Daten mit einer Aktualisierungszeit von 20 ms (bei Einsatz von Bluetooth) führt. Im Detail beinhalten die Funktionsblöcke folgende Mechanismen:

Vorverarbeitung und Zwischenspeicherung der Telegramme

Ziel der Telegramm-Vorverarbeitung ist es, die Funkstrecke zeitlich möglichst wenig zu belegen und eine Entkopplung von Kabelschnittstelle und Funkmedium zu erreichen. Dazu werden alle DP-Telegramme an die und von den topologisch nach der Funkstrecke angeordneten Profibusteilnehmer in einer Datenbank der Funktionsblöcke zwischengespeichert und auf Redundanz und Zeitstempel analysiert. Das sichert sowohl den Weiterbestand des Bus-Zeitverhaltens (bei Profibus bis zu 1,5 Mbit/s) auch bei Funkstörungen als auch die Verwendung von standardmäßigen Funktechnologien.

Durchlass von benötigten und Blockade von nicht benötigten Telegrammen

Ein Feldbus-Master sendet die DP-Daten zyklisch (bei 1,5 Mbit/s liegt die Zykluszeit unter 1 ms) an die Slaves, auch wenn sich der Dateninhalt nicht ändert. Diese Profibus-Telegramme werden von den Funktionsblöcken als immer gleich (redundant) erkannt und zur Entlastung der Funkstrecke herausgefiltert. Erst bei einer Änderung der Daten werden die Telegramme wieder durchgelassen und über Funk übertragen. In diesem Fall beträgt die Profibus-Aktualisierungszeit nach der Funkstrecke etwa 20 ms.

Zeitliche Bus-Arbitrierung

Da es auf der Funkstrecke zu Verzögerungen bei der Datenübertragung kommen kann, sollen Profibus-Telegramme erst dann gesendet werden, wenn der Master in seinem Zyklus den entsprechenden Teilnehmer anspricht. Bis zu diesem Zeitpunkt erfolgt eine Zwischenspeicherung der Telegramme. Ohne diese Arbitrierung wären regelmäßige Busfehler kaum zu vermeiden.

Aufbereitung der Funk-Telegramme auf Schlupffreiheit

Ein Feldbus-Telegramm wird für die Übertragung per Funk in unterschiedliche Funktelegramme eingebettet, die hintereinander gesendet werden. Funktechnologien garantieren für diese Prozedur grundsätzlich keine Schlupffreiheit. Als Gegenmaßnahme nimmt der Funktionsblock eine schlupffreie Wiederaufbereitung der Telegramme nach der Funkübertragung vor. Die Ausgabe der Telegramme erfolgt dann ohne zeitliche Lücke zwischen zwei Zeichen auf der Kabelschnittstelle.

Kommunikations- und Fehlersteuerung

Funktechnologien erzeugen allgemein komplexe Fehlerbilder. Bei einer Bitfeh-

lerrate von 10^{-3} enthält jedes 1.000ste Bit – das heißt im Mittel jedes zehnte DP-Telegramm – Datenfehler. Der Funktionsblock erkennt diese Fehlerbilder und korrigiert sie zum Beispiel über zusätzlich übertragene Datenlängeninformationen und Checksummen (etwa mit Forward Error Correction).

Verwaltung der FDL- und Token-Telegramme

Die im Broadcast Mode vom Master regelmäßig gesendeten FDL-Telegramme (Fieldbus Data Link) und Token-Telegramme dienen der Zuweisung von Kommunikationszeiten (Slots) an andere, am gleichen Bus befindliche Master wie Bedienstationen, weitere Steuerungen oder Programmiergeräte. Um solche nach der Funkstrecke angeordnete aktive Master bedienen zu können, arbeitet der Funktionsblock in diesem Fall wie ein Profibus-Multimaster. Die beiden Funktionsblöcke auf Master- und Slave-Seite nehmen stellvertretend für die Teilnehmer nach der Funkstrecke die Token an und bearbeiten sie auch stellvertretend (Token-Spiegelung).

Einstellung und Überwachung einer Filterzeit

Die aktive Ausfilterung von kurzen Funkstörungen innerhalb eines einstellbaren Zeitfensters verhindert die Generierung eines Busfehlers und damit einen Anlagenstillstand. Längere Funkstörungen dagegen werden als solche erkannt und von der Steuerung als Profibusfehler abgearbeitet. In diesem Fall reagiert die Steuerung gewollt wie bei einer gestörten Kabelverbindung und aktiviert alle für diesen Fall vorgesehenen Sicherheitsfunktionen in der Anlage. Die Filterzeit und damit die Grenze zwischen „Ausfiltern“ und „Passieren lassen“ ist zwischen 100 ms und 20 s einstellbar.

Ertüchtigung zum Funkstrecken-Diagnose-Tool

Zur Langzeitüberwachung und Diagnose der Funkstrecke wird das Funkmodul über den Funktionsblock zu einem eigenständigen Feldbus-Teilnehmer mit eigener GSD ertüchtigt. Über die GSD wird das Funkmodul in das Automatisierungssystem eingebunden, wodurch aus dem Programmablauf heraus auf die Funkstrecke beziehungsweise deren Status-Daten, wie Zykluszeiten, Fehlerzustände oder Wiederholversuche, zugegriffen werden kann. Diese Lösung ist wesentlich leistungsfähiger und universeller als beispielsweise Diagnoseanzeigen über LEDs.

Intelligente Abläufe im Funktionsblock

Bild 1 zeigt die im DE vorhandenen Funktionsblöcke zur Daten-Vorverarbeitung (blau) und Daten-Funkübertragung (orange) sowie als Beispiel den zeitlichen Ablauf einer Profibus/Profisafe-Kommunikation über eine Funkstrecke. Die Zeitachse verläuft von oben nach unten; die unten angeordneten „Klammern“ bezeichnen die verschachtelten Kommunikationsebenen zwischen Steuerungs- und Geräteseite. Als Beispiel für die Funktionsweise des Mechanismus dient die „schonende Belegung der Funkstrecke“:

Ein Master-Telegramm (schwarzer Pfeil oben links) der Steuerung erreicht den FB-DE (blau), wird von diesem zum integrierten Funkmodul auf der Master-Seite (orange) geleitet, dort in Funktelegramme verpackt sowie über die Funkstrecke zum Partnerfunkmodul auf der Slave-Seite und von diesem an den zweiten FB-DE geschickt. Dort wird das Funktelegramm schlupffrei aufbereitet und zum Profibus-Slave geschickt. Der Slave antwortet (grauer Pfeil), das Telegramm wird in gleicher Weise ver- und entpackt und nach der durch die Funkübertragung definierten Verzögerungszeit vom FB-DE an die Steuerung geschickt.

Zwischenzeitlich eintreffende, unveränderte (daher weiterhin schwarze) Telegramme des Master werden zur Entlastung der Funkstrecke abgeblockt und mit ebenfalls unverändert belassenen (grauen) Antworttelegrammen an die Steuerung beantwortet. In gleicher Weise wird zum einen der Slave vom rechten FB-DE weiterhin mit unveränderten Telegrammen versorgt, und zum anderen die entsprechende (graue) Slave-Antwort entgegen genommen, ohne die Funkstrecke zu belasten. Dieser Zustand dauert bis zum Eintreffen eines Master-Telegramms mit geändertem Inhalt (hellgrüner Pfeil). Jetzt wird erstmalig die Funkstrecke wieder belegt und der gleiche Ablauf bis zur Rücksendung des dunkelgrünen Antworttelegramms gestartet. Gleiches gilt für das dritte neue Telegramm (rot) und die zugehörige Antwort (orange).

Durch diese Entkopplung der Kabelschnittstelle vom Timing der Funkstrecke lassen sich Feldbusse wie Profibus ohne Busfehler über eine Funkstrecke betreiben.

Bild 2. Ein Beispiel für den praktikablen Einsatz von Wireless-Technologien ist der Ersatz von Schleppkabeln durch Funkstrecken bei mobilen Großgeräten wie Abräumer im Kohle-Tagebau, wobei angesichts des für Kabel und Trommel erforderlichen Aufwands Einsparungen im vierstelligen Euro-Bereich realisierbar sind. Weitere Einsatzbereiche für den Ersatz von Schleppkabeln oder Schleifkontakten sind zum Beispiel Kläranlagen und alle Arten von Kran- und Hebeeinrichtungen. (alle Bilder: Schildknecht)

Profisafe über Funkstrecken

Transparente Funkstrecken in Profibus-Systemen verhalten sich wie ein Kabel und sind daher ohne Änderungen am Projekt oder Verlust an Funktionalität einsetzbar. Dadurch wird auch die Verwendung von Profisafe, dem Sicherheitsprofil von Profibus und Profinet, in mit Funkstrecken ausgerüsteten Profibus-Netzen möglich. Profisafe läuft oberhalb der DE-Funktionsblöcke und überwacht, ob die Funkstrecke eine oder mehrere der folgenden Fehlerfälle generiert:

- Wiederholung, Verzögerung oder Verlust von Nachrichten
- Einfügung oder falsche Reihenfolge von Nachrichten
- Verfälschung von Daten und Vertauschung von Teilnehmern
- Wiederkehrende Speicherfehler in Switches

Durch die verschiedenen Mechanismen der Funktionsblöcke lassen sich alle genannten Fehlerfälle mit Ausnahme der Verzögerung von Nachrichten abfangen. Hier ist das Zeitverhalten der Funkstrecke mit der deutlichen Verlängerung (mindestens um den Faktor 10) und fehlenden Konstanz der Zykluszeit im Bereich nach der Funkstrecke zu beachten. Das ist von großer Bedeutung, da Profisafe über eine eigene Zeitüberwachung verfügt und Übertragungspausen ab einer bestimmten Länge als sicherheitsrelevant bewertet.

Grundsätzlich arbeitet Profisafe nach dem Black-Channel-Prinzip, wonach die Übertragungsstrecke selbst keinen Einfluss auf die Sicherheit hat. Diese wird vielmehr durch Überprüfungsmechanismen in der F-Steuerung und den angeschlossenen Profisafe-Geräten gewährleistet. Zu diesen Mechanismen gehört auch die maximal erlaubte Antwortzeit der Telegramme beziehungsweise deren Überprüfung. Die Länge dieser Überwachungszeit ist bei der Projektierung an die durch die Funkstrecke verlängerte Zykluszeit anzupassen. Kurzzeitige Funkstörungen werden durch eine Sicherheitsfunktion des Funktionsblocks in einem zwischen 100 ms und 20 s einstellbaren Zeitfenster überbrückt und damit bezüglich Profisafe unwirksam gemacht. Verzögerungen oberhalb dieses Zeitfensters führen zu einem gewollten Ansprechen der Sicherheitsfunktion mit Stillstand der Anlage. Praktische Erfahrungen zeigen, dass hierfür eine Erhöhung der Standardzeit für Not-Stopp von 500 ms auf 800 ms erforderlich ist. Es liegt dann jedoch am Anwender, zu prüfen, ob diese Verlängerung noch innerhalb der vom TÜV oder anderen Stellen vorgegebenen Sicherheitsanforderungen bezüglich der zu erfüllenden Reaktionsgeschwindigkeit der Anlage liegt.

Bluetooth am robustesten

Für Safety-Funkstrecken ist die Wahl der Funktechnologie naturgemäß von hoher Bedeutung. Bluetooth (BT) ist momentan die robusteste Funktechnologie, die es für den Einsatz in der Automatisierungstechnik gibt. Sie springt auf 79 Kanälen und verwendet mit 2,405 bis 2,488 GHz den gleichen Frequenzbereich wie WLAN. Während BT in seiner Ausprägung mit 1 mW Sendeleistung (Klasse 3) vorwiegend bei Konsumgütern wie Mobiltelefonen für kurze Distanzen zum Einsatz kommt, wird für die industrielle Nutzung dagegen BT-Klasse 1 mit einer bis zu 100 mW einstellbaren Sendeleistung verwendet, womit auch alle Anforderungen der neuen EN 300328 Version 1.8.1 erfüllt sind.

Zwar ist der Datendurchsatz bei Bluetooth geringer als bei WLAN; seine besondere Stärke ist jedoch das Frequenzsprungverfahren, wobei 1600 Frequenzwechsel pro Sekunde nach einem für jede Funkstrecke individuellen Muster erfolgen und so den Betrieb vieler unabhängiger Funkstrecken auf engem Raum ohne gegenseitige Beeinträchtigung erlauben. Durch dieses Frequency Hopping lässt sich BT auch nicht durch WLAN stören. Im Gegenzug besteht die Möglichkeit, bestehende WLAN-Netze durch das Konzept des Blacklisting (manuelle Einstellung zum Freihalten von bereits belegten WLAN-Kanälen) vor Beeinflussung durch BT zu schützen. *gh*

Thomas Schildknecht
ist Vorstand der gleichnamigen Schildknecht AG.