Adressierungssicherheit von Kommunikationsprotokollen

Anforderungen und wirksame Maßnahmen

Die Anwendung der IEC 61508 und der IEC 61784-3 für die sicherheitsgerichtete Kommunikation stellt besondere Anforderungen an die Kommunikationsprotokolle. Der vermehrte Einsatz solcher Kommunikationsprotokolle verlangt nach wirksamen Maßnahmen. Ebenso wichtig ist es, die Anwender für den sicheren Einsatz zu sensibilisieren. Die Qualität solcher Maßnahmen innerhalb der Protokolle muss sich an dem zu erreichenden Sicherheitslevel orientieren. Der Beitrag beschreibt die aktuellen Erkenntnisse zu diesem Thema.

SCHLAGWÖRTER Sicherheitsgerichtete Kommunikation / Profisafe / IEC 61508 / IEC 61784-3

Safety using Profisafe
The effectiveness of safety measures within communication protocols

Applying IEC 61508 and IEC 61784-3 for safety-oriented communications places high demands on the communication protocols. Increased use of safety related protocols calls for effective measures. It is equally important to sensitize the users. The quality of such measures within the protocols must be appropriate for the requirements of the required safety level.

KEYWORDS Safety-related communications / Profisafe / IEC 61508 / IEC 61784-3

HEINRICH-THEODOR HANNEN, JOSEF BÖRCSÖK, Universität Kassel

Die sicherheitsgerichtete Prozessdatenkommunikation ist in den letzten 15 Jahren immer mehr ein Baustein der Automatisierungs- und Prozesstechnik geworden. Anfangs waren es nur wenige Anwendungen und Protokolle, die auf Feldbussen eingesetzt wurden. Bis heute ist die Anzahl der Protokolle beträchtlich gewachsen. Sie setzen nun vermehrt auf Ethernet-basierte Übertragungstechniken, wodurch sich eine Vielzahl verschiedener Technologien und Medien für die Übertragung nutzen lassen. Mit Sicherheit, safety, ist in diesem Beitragdie funktionale Sicherheit gemeint, wie sie die IEC 61508-4 [1] definiert.

Aktuelle Sicherheitsprotokolle orientieren sich an der IEC 61508-2 und im Besonderen an der IEC 61784-3. Letztere beschreibt die Gefahren für die Kommunikation und die Anforderungen, die die Sicherheitsprotokolle diesbezüglich beherrschen müssen. Zu den klassischen Gefahren für die Sicherheit von Nachrichten [2] zählen

- Verfälschungen
- unerwünschte Wiederholungen
- Reihenfolgevertauschungen
- Einfügungen (einzelner Telegramme und Sequenzen)
- Verlust
- Verzögerung
- Fragmentierung
- Maskierung
- falsche Adressierung

1. AUFLAGEN FÜR DEN ANWENDER

Neben den Gefahren aus der IEC 61784-3 wurden in [8] weitere Gefährdungen für sicherheitsgerichtete Protokolle aufgezeigt. Danach sollten Anwender solcher Protokolle Maßnahmen ergreifen, die folgende Bereiche abdecken:

- Absichtliche Unterminierung der Sicherheitsmechanismen
- Fehlerhafte Konfiguration
- Absehbarer Missbrauch
- Absehbare Fehlbedienung
- Unberechtigter Zugriff
- Gefährdungen durch offene Übertragungssysteme

Diese Gefahren werden von den heute verwendeten Protokollen meist nicht adressiert, da sich der Schutz durch ein Bündel von organisatorischen und technischen Maßnahmen außerhalb der Geräte, die die Sicherheitsprotokolle realisieren, erreichen lässt. Die entsprechenden Hinweise in den Sicherheitshandbüchern der Gerätehersteller helfen jedoch dem Anwender. Zum Beispiel müssen die Themen absehbarer Missbrauch und Fehlbedienung in den heute gängigen Anwendungsbereichen beachtet werden, da die üblichen Einschränkungen der Sicherheitsprotokolle auf „geschlossene Übertragungssysteme“, das heißt solche, die diese Gefährdung ausschließen, nur bedingt mit dem Einsatzgebiet vereinbar sind.

Besonders bei Verwendung Ethernet-basierter Übertragungssysteme sind umfangreiche Gefährdungspotenziale zu betrachten. Hierbei sind mindestens ein oder mehrere PCs samt PC-Betriebssystem im Netzwerk vorhanden. Diese der Steuerungsebene nahen PCs sind mit Rechnern der Produktionsplanung und -steuerung verbunden und somit bis hinauf in die Unternehmens-IT integriert. Für die Steuerungsebene sind die Möglichkeiten der Fernwartung ebenfalls relevant. Nicht zu vergessen temporär anwesendes Wartungspersonal des Herstellers oder Betreibers mit mobilen PCs, die Zugriff auf sicherheitsgerichtete Komponenten erhalten.

2. NACHRICHTENVERFÄLSCHUNGEN

Die klassischen Gefahren für sicherheitsgerichtete Protokolle stellen für die Definition von Protokollen eine Herausforderung dar. So ist das Aufdecken einer Nachrichtenverfälschung mit SIL3-Qualität [1] für eine Si-

cherheitsfunktion mit einer Restfehlerrate von 10^{-9}/h [2] nicht einfach, wenn als Übertragungssystem der Black-Channel-Ansatz [1] gewählt wird. Dieser macht es erforderlich, für jede Bit-Fehlerwahrscheinlichkeit von kleiner gleich 10^{-2} die Verfälschung einer Nachricht mit geeigneter Qualität aufdecken zu können. Deshalb musste die erste Version des Protokolls CIP-Safety Ed. 1.1 [5] verbessert werden, um qualitativ geeignete Maßnahmen für die Erkennung von Nachrichtenverfälschungen zu erreichen. Auch bei der Portierung von Profisafe V1 (für Profibus) [4] auf V2 für Profinet wurden größere CRC benutzt.

Selbst bei einem 32-bit-CRC und den von Profisafe verwendeten Nutzdatenlängen von bis zu 123 Bytes ergibt sich eine SIL3-konforme Restfehlerrate erst bei einer Bit-Fehlerwahrscheinlichkeit von etwa 10^{-4}. Wegen diesem Problem führte Profisafe den patentrechtlich geschützten SIL-Monitor [3] ein. Dieser Mechanismus löst die Sicherheitsreaktion aus, wenn vom Standard-Übertragungssystem Profibus oder Profinet eine Nachricht an Profisafe weitergegeben wird, die einen erkennbaren Profisafe-CRC-Fehler aufweist. Der Mechanismus führt dazu, dass die Verfügbarkeit einer Profisafe-Verbindung gegenüber einem Protokoll, das bei Vorliegen von CRC-Fehlern des Sicherheitsprotokolls keine Sicherheitsreaktion benötigt, reduziert ist, falls unterlagerte Mechanismen, wie zum Beispiel Profinet oder Profibus-DP, diese Fehler nicht aufdecken. Dies ist bei Nachrichtenverfälschungen und im Rahmen von eingefügten Nachrichten interessant, weil diese ebenfalls zu einem CRC-Fehler führen. Die mögliche verfügbarkeitssteigernde Implementierung, für eine begrenzte Zeitspanne einen CRC-Fehler zu tolerieren [3], wird von den meisten eingesetzten Realisierungen nicht genutzt.

3. EINFÜGUNGEN

Eine verbreitete Schwäche von sicherheitsgerichteten Protokollen ist die Beherrschung von eingefügten Nachrichten mit einer für SIL3 geeigneten Restfehlerrate. So verwendeten Profisafe V1 [4], FF-SIF [7] und CIP-Safety Edition 1.1 [5] alle einen 16-bit-Zähler (Consecutive-Number, Macro-Cycle-Number, Time-Stamps). Dies wurde in Nachfolgeversionen der Protokolle verbessert, sodass beispielsweise Profisafe V2 [3] nun einen 24-bit-Zähler verwendet. Dieser Wandel rührt daher, dass das Bewusstsein für die geforderte Qualität der Maßnahmen in den Protokollen erst allmählich das Denken der Protokollentwickler beeinflusst hat, wenngleich die Forderung aus der IEC 61508 von Beginn an bestand.

Besondere Beachtung verdient das Thema Einfügungen von Nachrichten durch die vermehrt eingesetzte Ethernet-Technologie. Die dabei verwendeten Hardware-Komponenten sind mit vergleichsweise großen Speichern ausgestattet, von denen anzunehmen ist, dass sie viele Nachrichten aufnehmen und zu einem späteren Zeitpunkt fälschlicherweise wieder versenden können. In einigen Ethernet-Ring-Technologien gehört das Speichern und erneute Senden zum Funktionsumfang nach einer Topologieänderung. Daraus entsteht die Gefahr, dass die Kommunikation nach einer Sicherheitsreaktion unbeabsichtigt anläuft.

Bei Profisafe besteht das Anlaufverhalten aus 3 Nachrichten, mit denen noch keine Prozessdaten aktiv werden, bevor dann mit der vierten der normale Betrieb aufgenommen wird. Durch diese 3+1 Nachrichten wird bei Profisafe die Restfehlerrate für einen unerwünschten Anlauf mit SIL3-Qualität verhindert, eine Rate P für das Einfügen einer einzelnen passenden Nachricht von kleiner $5{,}62 \cdot 10^{-3}$/h vorausgesetzt. Damit gilt $P^4/h \leq 10^{-9}/h = 1\,\%$ von SIL3.

Das beschriebene Verhalten betrifft den Wiederanlauf des initialen Zustands von Profisafe, beispielsweise nach Power-On. Im Falle des Wiederanlaufs nach einer Sicherheitsreaktion sind aufgrund der Verzögerung durch das Operator-Acknowledge im F-Host weitere passende Nachrichten erforderlich, die die Restfehlerrate noch verringern. Dies ist ein vergleichsweise guter Mechanismus für sicherheitsgerichtete Kommunikationsprotokolle, zumal nicht sicherheitsgerichtete Mechanismen in Profinet einen Teil dieser Fehler ebenfalls beherrschen.

4. ADRESSIERUNGSSICHERHEIT

Eine falsche Adressierung lässt sich mit zwei Verfahren aufdecken.

Verbindungs-Identifikation
Das erste Verfahren definiert für eine sicherheitsgerichtete Kommunikationsverbindung eine dieser Verbindung zugeordnete eineindeutige ID (Nummer). Anhand dieser Nummer erkennt der Empfänger, ob dies eine Sendung für die bei ihm vorhandene Kommunikationsverbindung ist. Damit die Richtung, in der die Nachricht versendet wird, eineindeutig ist, gibt es in der Nachricht ein weiteres Kennzeichen (siehe zum Beispiel FF-SIF [7]).

Absender-Empfänger-Identifikation
Das zweite Verfahren definiert für die Kommunikationspartner in einem sicherheitsgerichteten Netzwerk Adressen (zwei Nummern), die innerhalb des Netzwerks eineindeutig sein müssen. Diese Nummern werden mit den sicherheitsgerichteten Nachrichten übertragen und ermöglichen es dem Empfänger zu erkennen, ob die Nachricht vom richtigen Absender stammt und für ihn bestimmt ist. Neben der Übertragung der Adressinformationen innerhalb der Nachricht gibt es ein patentiertes Verfahren, bei dem die Adressinformationen nicht übertragen werden, jedoch in die Berechnung des CRCs eingehen, sodass die Empfänger

dies auf Grund ihrer Erwartungshaltung überprüfen können. Dieses Verfahren wendet Profisafe an.

4.1 Qualifizierung der Adressierung

Ob die jeweilige Adressierungstechnik sich eignet, hängt von den Datengrößen der verwendeten Nummern ab. Wenn die Nummern durch die CRC-Berechnung ersetzt werden, kann für die Qualifizierung der Adressierungstechnik höchstens die Größe des CRCs herangezogen werden, auch dann, wenn die eingesetzten, nicht übertragenen Nummern, größer sind. Dies trifft für Profisafe zu. Hier werden für den F-Host 16 bit und weitere 16 bit für das F-Device verwendet, die jedoch wieder auf einen 16-bit-CRC-Preset (CRC1 von Profisafe) „heruntergerechnet" werden, sodass nur etwa 2^{16} verschiedene Identifikationen zum Einsatz kommen. Da neben den Adressen bei Profisafe noch weitere Daten aus den F-Parametern mit in die CRC-Berechnung eingehen, kommt es vor, dass für zwei unterschiedliche Adresspaare der selbe CRC-Preset berechnet wird, ohne dass der Anwender darauf einen Einfluss hätte. Hierbei wird nicht die Wirksamkeit des Profisafe-CRC-Verfahrens in Frage gestellt, sondern nur die eineindeutige Adressierung durch den Preset betrachtet.

Falls eine solche Situation aufgrund der Anlagenkonfiguration gegeben ist, besteht für die Kommunikationsverbindungen mit identischem Preset die Gefahr, dass sich die Profisafe-Nachrichten nicht mehr eineindeutig einer Verbindung zuordnen lassen. Dies ist relevant, wenn sie von der unterlagerten Transportschicht an den falschen Empfänger, dem derselbe Preset zugeordnet ist, versendet werden. Ebenso ist es denkbar, dass die Profisafe-Nachrichten und die zugehörigen F-Parameter von unterschiedlichen F-Modulen stammen, da ein F-Modul zwar die zu ihm passenden F-Parameter anhand der darin enthaltenen F-Adresse prüfen kann, aber die Authentizität der Profisafe-Nachrichten eben nur durch den Preset für die CRC-Rechnung erkennbar ist.

Es gibt einen Sonderfall, bei dem der CRC-Preset aller F-Module immer unterschiedlich ist. Dazu darf im Netzwerk nur ein F-Host definiert sein und die F-Parameter der F-Devices dürfen sich nur in der F-Device-Adresse unterscheiden. Parameter, wie zum Beispiel F_WD_Time, müssen bei allen Verbindungen zu den F-Modulen gleich sein. Weiterhin dürfen dann die F-Module keinen iPAR-CRC verwenden. Da sich in diesem Fall nur die 16-bit-F-Device-Adressen in den F-Parametern unterscheiden, berechnet ein 16-bit-CRC immer einen unterschiedlichen CRC-Preset.

4.2 Symmetrische Adressdekodierung

Eine entscheidendere Schwachstelle der Adressierungstechnik von Profisafe ist, dass die „Adresse", das heißt der CRC-Preset für Nachrichten vom F-Host an das F-Device und von diesem zurück zum F-Host identisch ist. Damit kann der F-Host eine von ihm generierte Nachricht nicht von der von einem F-Device stammenden Nachricht unterscheiden, wenn die Datenlänge für Eingangsdaten und Ausgangsdaten gleich ist. In diesem Fall ist die Nachricht des F-Hosts eine gültige F-Device-Antwort. Ein Fehler an dieser Stelle führt dazu, dass der F-Host falsche Eingangsdaten benutzt und dass die Überwachungszeit (F_WD_Time) nicht abläuft, obwohl keine Nachricht vom F-Modul beim F-Host eintrifft.

Für das F-Device stellt im genannten Fall die eigene Nachricht solange eine gültige Wiederholung dar, bis die Überwachungszeit (F_WD_Time) abgelaufen ist oder eine neue Nachricht vom F-Host empfangen wird. Die neue Antwort auf die Nachricht des F-Hosts stellt wieder eine gültige Wiederholung dar. Da es Profisafe zulässt, dass die Daten einer Wiederholung geändert sein dürfen und diese geänderten Daten verwendet werden dürfen, benutzt das F-Device für maximal F_WD_Time falsche Ausgangsdaten.

Eine solche Situation kann durch einen Fehler im Standard-Übertragungssystem entstehen, wozu auch die Backplane und die Busanschaltung der Sicherheits-SPS und Ein-/Ausgangskomponenten gehören. Sehr einfach ist der Fehler zum Beispiel im Profinet/Profibus-Protokollstack eines Standard-Feldbuskopplers denkbar, bei dem die Adresse, die für die Output-Daten des F-Moduls verwendet werden soll, fälschlicherweise auf die Input-Daten desselben F-Moduls gesetzt wird, während die Profisafe-Verbindung etabliert ist. Dabei muss es sich nicht zwingend um Softwarefehler handeln, auch die Busanschaltungen mit einem Profibus-Chip oder einem Profinet-Chip könnten derartige Fehler verursachen, da auch in ihnen die Daten für F-Input und F-Output gespeichert sind.

Der einfachste Fall ist zum Beispiel ein Dual-Port-Ram, das als Schnittstelle zwischen Busanschaltung und dem F-Modul dient. Liegen die Datenbereiche für F-Input- und F-Output-Daten auf Adressen, die sich nur durch eine oder einige wenige Adressleitungen unterscheiden, beispielsweise weil das Dual-Port-Ram zur Hälfte für F-Input und zur anderen Hälfte für F-Output-Daten genutzt wird, reicht im ungünstigsten Fall schon ein einfaches Stuck-At an einer Adressleitung des Dual-Port-Rams aus, um den Fehler herbeizuführen.

Ein weiterer Fehler kann durch die Diagnosefunktionen von Ethernet-Bausteinen entstehen. Die Bausteine ermöglichen es zu Testzwecken, die ausgehenden Nachrichten nach innen zu spiegeln. Werden beispielsweise Loop-Back-Testeinrichtungen durch die Parametrierung eines Mirror-Ports zu Wartungszwecken aktiviert, könnte die Sicherheits-SPS eine von ihrer Profinet-Anschaltung versendete Nachricht wieder „empfangen". Wenn nun auch die Profinet-Mechanismen die Nachricht gültig erscheinen lassen würden (was sie in der Regel nicht tun) würde sie dem Profisafe-Protokoll zu-

gestellt. Aus sicherheitstechnischer Sicht wurden die Mechanismen von Profinet nicht für die Betrachtung herangezogen, da der Anspruch nach Einsatz des Black-Channel-Prinzips besteht.

Es bleibt festzustellen, dass die Adressierungssicherheit bei Profisafe aufgrund des hier beschriebenen, vom Profisafe-Protokoll unerkannten Fehlers, risikomindernde Eigenschaften der unterlagerten Standard-Komponenten mit in die Sicherheitsbetrachtung einbeziehen muss. Diese Informationen sind der zuständigen Nutzerorganisation mitgeteilt und im Profisafe-Arbeitskreis diskutiert worden. Es wurde vereinbart, dass die Hersteller die Relevanz der Adressierungssicherheit für ihre Geräte untersuchen.

Die Ergebnisse der durch die PNO veranlassten Untersuchungen ergaben, dass die Restfehlerrate für den betrachteten Adressierungsfehler hinreichend klein ist, sodass die Anforderungen gemäß dem Safety-Integrity-Level 3 der IEC 61508 erreicht werden. Der Arbeitskreis plant jedoch, in einer künftigen Version des Protokolls Profisafe eine verbesserte Adressierungstechnik zu spezifizieren

5. FAZIT

Sicherheitsgerichtete Protokolle und deren Einsatz im industriellen Umfeld stellen eine komplexe Materie dar. Selbst bei einfachen Protokollen wie Profisafe werden selbst nach Jahren und nach zahlreichen Prüfungen Schwächen festgestellt. Bis heute fehlen noch allgemein akzeptierte Fehlerraten, zum Beispiel für das Einfügen und Wiederholen von Nachrichten, die eine standardisierte Qualifizierung von Maßnahmen ermöglichen würden.

MANUSKRIPTEINGANG
21.02.2011
Im Peer-Review-Verfahren begutachtet

AUTOREN

Dipl. Inform. **HEINRICH-THEODOR HANNEN** (geb. 1962) ist Doktorand der Universität Kassel (Fachgebiet Rechnerarchitektur und Systemprogrammierung) im Fachbereich 16 – Elektrotechnik/Informatik). Er ist seit mehr als 14 Jahren auf dem Gebiet der Sicherheitsrechnertechnik tätig und arbeitet in nationalen und internationalen Gremien mit an der Definition sicherheitsgerichteter Kommunikationsprotokolle.

Universität Kassel,
Fachgebiet – Elektrotechnik/Informatik im Fachgebiet Rechnerarchitektur und Systemprogrammierung,
Wilhelmshöher Allee 73, D-34109 Kassel,
Tel. +49 (0) 561 804 65 85, E-Mail: h.hannen@uni-kassel.de

Prof. Dr.-Ing. habil. **JOSEK BÖRCSÖK** (geb. 1959) ist Professor an der Universität Kassel (Fachgebiet Rechnerarchitektur und Systemprogrammierung) im Fachbereich 16 – Elektrotechnik/Informatik). Er ist seit mehr als 11 Jahren auf dem Gebiet der Sicherheitsrechnertechnik tätig und arbeitet in nationalen Gremien des DKE und internationalen Organisationen mit.

Universität Kassel,
Fachgebiet – Elektrotechnik/Informatik im Fachgebiet Rechnerarchitektur und Systemprogrammierung,
Wilhelmshöher Allee 73, D-34109 Kassel,
Tel. +49 (0) 561 804 65 85, E-Mail: j.boercsoek@uni-kassel.de

REFERENZEN

[1] IEC 61508, "Functional safety for electrical/electronic/programmable electronic safety related systems", parts 1 – 7, 2010

[2] IEC 61784-3, Industrial Process Measurement and Control, Part 3: „Profiles for functional safety communications in industrial networks – General rules and profile definitions", CD Edition 2.0, 2008

[3] PROFIBUS INTERNATIONAL, PROFIBUS Specification: „Profisafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO", V2.5c, February 2010

[4] PROFIBUS INTERNATIONAL, PROFIBUS Specification: „Profisafe – Profile for Safety Technology", V1.30, June 2004

[5] Open DeviceNet Vendors Association, "The CIP Networks Library", Volume 5, „CIP Safety", Ed. 1.1, 2006, www.odva.org

[6] Open DeviceNet Vendors Association, "THE CIP Networks Library", Volume 5, „CIP Safety", Ed. 2.2, 2008, www.odva.org

[7] Foundation Specification: "FF-SIF Protocol Specification", Revision FS1.1, July 13, 2007

[8] Hannen, H.-T., "Analyse sicherer Kommunikationsprotokolle im industriellen Einsatz", Dissertation an der Universität Kassel im Fachbereich 16 – Elektrotechnik / Informatik im Fachgebiet Rechnerarchitekturen und Systemprogrammierung, 2011 i.A.