phoenixcontact.de/channel-prinzip

KNOW-HOW IN SAFETY
by GIT SICHERHEIT & PHOENIX CONTACT

Diesmal im Fokus:

Black Channel-Prinzip

Lutz Rahlves, Product Marketing Safety

Die IEC 61508 definiert den Begriff „Black Channel". In der Kommunikationstechnik versteht man darunter einen Kommunikationskanal mit ungesicherten oder nicht anwendungsspezifischen Eigenschaften. Der „Black Channel" ist ein kennzeichnendes Element des „Black Channel-Prinzips", bei dem trotz der genannten Ausgangseigenschaften eines Kommunikationskanals eine sichere Kommunikation gewährleistet werden soll.

Im Umfeld der funktionalen Sicherheitstechnik geht es dabei hauptsächlich um die Übertragung von sicherheitsgerichteten Signalen über standardisierte Kommunikationsmedien (z. B. Ethernet oder WLAN). Grundsätzlich werden sicherheitsgerichtete Signale von A nach B übertragen. Das kann z. B. ein Signal von einer Not-Halt-Einrichtung sein, das zur sicheren Steuerung übertragen werden soll. Der Wunsch liegt nahe, dass die sicherheitsgerichteten Signale gemeinsam mit den Standardsignalen über ein gemeinsames Netzwerk transportiert werden.

Es geht also um die Integration der funktionalen Sicherheitstechnik in das bestehende Netzwerk. Auf diese Weise lässt sich u. a. ein zusätzlicher Verdrahtungsaufwand vermeiden und Kosten minimieren. Doch die bereits bestehenden Netzwerke sind in der Regel nicht nach den Anforderungen der funktionalen Sicherheit entwickelt worden, wodurch es zu verschiedenen Fehlerfällen wie die Wiederholung, den Verlust oder die Verzögerung von Telegrammen (Dateneinheiten aus Nutz- und Steuerdaten) kommen kann.

Wie kann man ein sicherheitsgerichtetes System nach den Anforderungen der IEC 61508 aufbauen?

Das bestehende Netzwerk verfügt über keinen ausreichenden Schutz, deshalb muss an dieser Stelle ein Sicherheitsprotokoll überlagert werden. Das Sicherheitsprotokoll läuft oberhalb vom Standardprotokoll. Es muss Mechanismen integrieren, um jeden möglichen Fehlerfall oder eine Kombination mehrerer Fehler zu erkennen und zu beherrschen. Mithilfe dieser fehlererkennenden Maßnahmen und der fehlenden Anforderungen an das übertragende Netzwerk kann man die Integrität der Datenübertragung über das Netzwerk überwachen.

Was passiert bei einer Fehlererkennung?

Sobald ein nicht-tolerierbarer Fehler erkannt wird, rechnen die Systeme nur noch mit Ersatzwerten. Konkret wird bei einer Störung in der Kommunikation in der sicheren Steuerung mit dem Ersatzwert „0" gerechnet. Dies kann z. B. bei einem sicheren Eingang mit nicht-betätigtem Not-Halt der Fall sein. Das bedeutet, es wird der sichere Zustand „0" angenommen, als wäre der Not-Halt betätigt worden. In der Ausgangsrichtung überwacht das Ausgangsmodul die Integrität der Daten. Wird hier ein Fehler detektiert, werden Ersatzwerte ausgegeben. In diesem Fall werden alle sicheren Ausgänge auf dem Modul abgeschaltet und die funktionale Sicherheit ist gewährleistet.

Diese Funktionalität ist auch bei einer Datenübertragung über Wireless-Verbindungen gegeben. Sobald das Netzwerk eine Übertragung z. B. über WLAN oder Bluetooth zulässt, werden die sicherheitsgerichteten Daten übertragen. Dabei muss man evtl. die reduzierte Bandbreite bzw. die längere Übertragungszeit berücksichtigen. Auch die standortübergreifende Übertragung der Safety-Signale über einen Cloud-Dienst ist möglich.

Autor
Lutz Rahlves
Product Marketing Safety
Phoenix Contact Electronics GmbH
Bad Pyrmont

Kontakt:

Phoenix Contact GmbH & Co.KG
Blomberg
safety-service@phoenixcontact.com
www.phoenixcontact.com