LONMARK® DEUTSCHLAND

Funktionale Sicherheit mit SAFETYLON®

WHITE PAPER

Einleitung

Viele Einrichtungen der Prozess- und Gebäudeautomation erfordern ein hohes Maß an Sicherheit. Weiträumig ausgelegte Netzwerke sind in der Lage, gefahrvolle Ereignisse zu signalisieren und im Zusammenwirken mit zahlreichen Sicherheitseinrichtungen geeignet zu reagieren. Diese „funktionale Sicherheit" hilft Gefahren abzuwehren oder gar Menschenleben zu schützen. Unter Federführung des LONMARK Deutschland e.V. und im Rahmen eines EU-Förderprojektes wurde von 2005 bis 2008 die SAFETYLON-Technologie entwickelt, welche Anwendungen mit funktionaler Sicherheit mit der LON-Technologie einfach, wirtschaftlich und leistungsfähig möglich macht.

Dieses White Paper gibt einen Überblick über die SAFETYLON-Technologie, schildert mögliche Einsatzszenarien, beschreibt die vorhandenen Entwicklungsergebnisse des EU-Förderprojektes, ordnet die Berichte und Zulassungen des TÜV Rheinland ein und gibt Herstellern Hinweise für eine erfolgreiche Implementierung dieser Technologie.

Inhalt

Einleitung	1
Motivation	1
Normen	2
SAFETYLON-Systemübersicht	2
Ein gemeinsames Netzwerk	3
Sicherer Datenverkehr	3
SCADA-Systeme	4
Einfache, sichere Produkte	4
Inbetriebnahme und Tests	5
Sichere Geräte	5
Sichere Firmware	6
Entwicklungsergebnisse	6
Produktentwicklung	7
Fazit	7

Motivation

Unter „Funktionaler Sicherheit" versteht man die zuverlässige und sicherheitsgerichtete Funktion von Systemen und Komponenten sowohl im Normalbetrieb als auch bei Ausfällen und Fehlern. Dabei müssen die entsprechenden nationalen und internationalen Standards und Normen (IEC 61508, IEC 61511 und weitere) angewendet und eingehalten werden. Die Motivationen zum Einsatz funktionaler Sicherheit sind vielfältig:

- Anerkannte Normen und Standards enthalten Vorgaben für Hersteller, Dienstleister und Betreiber, um das Risikopotential möglichst klein zu halten.
- Hersteller von sicherheitsrelevanten Produkten möchten Vorreiter sein und sich so von Wettbewerbern abheben.
- Forderung von Projektverantwortlichen (beispielsweise Investoren oder Planer) für einzelne Projekte und einzelne Funktionen.

„SIL 3-Applikationen mit vielen Komponenten und hohen Datentransferraten sind möglich."

Normen

Zurzeit gibt es diese, für die LON-Technologie relevanten und auf die Basisnorm IEC 61508 beziehende Anwendungsbereiche und Normen[1]:

Anwendungsbereich	Normen[2]
Bahnanwendungen	DIN EN 50126, DIN EN 50128
Beleuchtungssysteme	DIN EN 50512
Feuerungsanlagen	DIN EN 50156-1
Gaswarnsysteme	DIN EN 50271, DIN EN 50402
Kernkraftwerke	DIN IEC 61513
Prozessindustrie	DIN EN 61511
Straßenverkehrs-Signalanlagen	DIN V VDE V 0832-500

Insgesamt ist eine zunehmende Tendenz zu erkennen, dass Anforderungen im Sinne der funktionalen Sicherheit in bestehende und neue Normen aufgenommen werden. Dies spiegelt die größer werdende Marktrelevanz im jeweiligen Segment wieder.

Unabhängig von existierenden Anwendungsnormen (C-Normen) spielt funktionale Sicherheit in vielen weiteren Bereichen eine große Rolle. Beispielhaft sind hier einige Anwendungen aufgeführt:

- Aufzugssteuerungen
- Branddetektion, -meldung und –schutz
- Messung von unverträglichen oder toxischen Stoffen
- Entrauchungs- und Rauchschutzdruckanlagen
- Fluchtweg-Managementsysteme
- Not- und Sicherheitsbeleuchtungssysteme
- Türsteuerungen
- Zugangskontrollsysteme

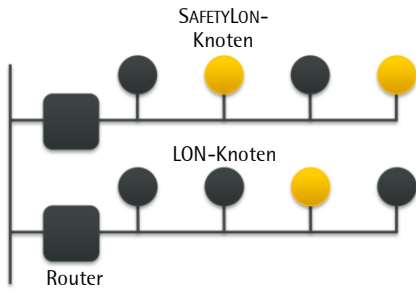

Abbildung 1: Sichere und nicht sichere Knoten in einem gemeinsamen Netzwerk

SAFETYLON-Systemübersicht

SAFETYLON-Netzwerke benötigen kein eigenes Netzwerk, sondern können in neuen und bestehenden LON-Netzwerken gemeinsam mit herkömmlichen LON-Knoten betrieben werden (Abbildung 1). Physikalisch getrennte Netzwerke sind daher nicht erforderlich. Neben dieser Einsparung ergibt sich der technische Vorteil, dass sowohl auf

[1] Diese Liste erhebt keinen Anspruch auf Vollständigkeit.
[2] U.U. existieren weitere Normen, die aus Platzgründen hier nicht erwähnt werden.

nicht sichere als auch sichere Daten innerhalb eines gemeinsamen Netzwerks zugegriffen werden kann. Durch die Verwendung der LON-Technologie für beide Bereiche ergeben sich sowohl auf der technischen Ebene, als auch für die Vermarktung, neue Möglichkeiten.

Ein gemeinsames Netzwerk

Der Transport sicherer und nicht sicherer Nachrichten innerhalb eines gemeinsamen Netzwerkes bietet viele Vorteile (Abbildung 2):

- Verwendung herkömmlicher Komponenten für den sicheren Datenverkehr
- Einfache Anbindung an das gleiche, gemeinsame SCADA-System
- Sichere und nicht sichere Anwendungen im gleichen Produkt

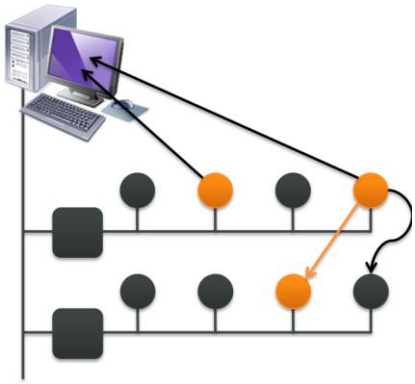

Abbildung 2: mit SAFETYLON werden sichere (gelb) und nicht sichere (grau)Nachrichten in einem gemeinsamen Netzwerk verteilt

Innerhalb des Netzwerkes können herkömmliche Leitungen verwendet werden. Normale Router oder Repeater können ebenso eingesetzt werden. Mit einem Visualisierungssystem können – wie bisher gewohnt – Lösungen erstellt werden. Auch die Verwendung herkömmlicher, dezentralisierter Visualisierungslösungen (beispielsweise embedded OPC) ist möglich. Optional können innerhalb eines SAFETYLON-Knotens vollkommen rückwirkungsfrei sichere und nicht sichere Applikationen betrieben werden.

Sicherer Datenverkehr

Normale Router oder Repeater (auch Physical Layer Repeater) können für den sicheren Datenverkehr genutzt werden. Dies wird dadurch ermöglicht, dass das sichere SAFETYLON-Protokoll als LON-Daten transportiert wird (Abbildung 3). Das SAFETYLON-Protokoll (gelb) wird innerhalb des LON-Protokolls (grau) als Datum versandt. Durch diese „Tunnelung“ des SAFETYLON-Protokolls können beliebige Infrastrukturkomponenten verwendet werden, weil diese Geräte den eigentlichen LON-Dateninhalt nicht beeinflussen.

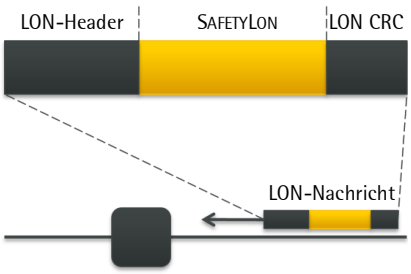

Abbildung 3: „Tunnelung“ des SAFETYLON-Protokolls

Das SAFETYLON-Protokoll hat eine sehr geringe Restfehlerwahrscheinlichkeit, so dass SIL 3-Applikationen mit vielen Komponenten und hohen Datentransferraten möglich sind. Durch den speziellen Aufbau jeder SAFETYLON-Nachricht bleiben auch extrem hohe Störeinflüsse ohne negative Wirkung auf die Güte und Verfügbarkeit. Aus diesem Grund können in SAFETYLON-Netzwerken herkömmliche Leitungen verwendet werden.

Abbildung 4: Eine Türsteuerung kann einen Zustand mit herkömmlichen Datentypen melden

SCADA-Systeme

Für das gemeinsame Netzwerk ist ein Visualisierungssystem ausreichend. Mit diesem lassen sich Datenpunkte von sicheren und herkömmlichen Komponenten verarbeiten. Ein sicherer Knoten kann dabei sowohl sichere als auch nicht sichere Datenpunkte empfangen oder senden.

Dies hat erhebliche Vorteile. So kann beispielsweise eine Türsteuerung mit einem sicheren Datentyp durch einen sicheren Sensor gesteuert werden und gleichzeitig kann die gleiche Türsteuerung für Visualisierungs- oder Diagnosezwecke den Zustand (offen oder geschlossen) mit herkömmlichen Datentypen an die Visualisierung melden (Abbildung 4). Auch der Empfang herkömmlicher Daten in einem sicheren Gerät kann sinnvoll sein.

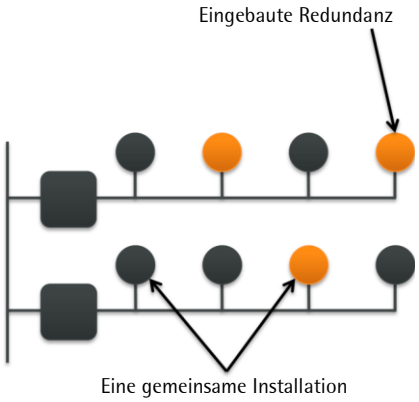

Abbildung 5: SAFETYLON-Produkte und -Netzwerke sind einfach aufgebaut

Einfache, sichere Produkte

SAFETYLON-Produkte sind einfach aufgebaut und können einfach installiert werden. Im Gegensatz zum Einsatz herkömmlicher Technik werden nicht zwei getrennte und aufwendig zu installierende Produkte benötigt, sondern eben nur ein SAFETYLON-Produkt. Dies spart genauso Kosten, wie die Vermeidung redundanter Installation durch die Verwendung einer einfachen Installation. Bei diesen Kosteneinsparungen kann man jedoch sehr viel mehr Sicherheit erreichen. So ist es mit der SAFETYLON-Technologie möglich, SIL 3-Anwendungen zu realisieren, während mit herkömmlicher Technik aufwendig und maximal nur SIL 2-Anwendungen umgesetzt werden können.

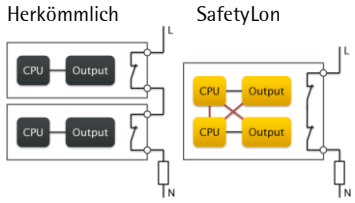

Abbildung 6: Redundanz im Vergleich

Anstelle von zwei Produkten kann ein SAFETYLON-Produkt verwendet werden. Der interne Aufbau ist unterschiedlich (Abbildung 6). Ein normales Produkt ist einkanalig aufgebaut und verfügt über eine CPU, welche beispielsweise den oder die Ausgänge steuert. Um die entsprechende Sicherheit zu gewährleisten, werden bei einem Ausgang die Relaiskontakte von zwei Produkten in Reihe geschaltet. So kann jedes Gerät unabhängig den Ausgang abschalten.

Ein SAFETYLON-Gerät hat diese Redundanz eingebaut, da es über zwei unabhängige CPUs und zwei unabhängige Ausgangskanäle verfügt (Abbildung 6). Da diese Redundanz sich in einer Elektronik befindet, können die einzelnen Schaltkreise sehr viel enger gekoppelt werden, als dies bei getrennten Geräten der Fall sein kann. So sind die CPUs direkt miteinander verbunden und überwachen sich gegenseitig. Jede CPU kann zudem jeden Ausgangskanal

unabhängig schalten. Daher erreicht man mit dem SAFETYLON-Design eine sehr viel höhere Diagnoseabdeckung und Sicherheit. Dies ist einer der Gründe, warum ein SAFETYLON-Gerät Anwendungen bis SIL 3 unterstützt.

Inbetriebnahme und Tests

Bei getrennten Netzwerken oder gar unterschiedlichen Technologien erfolgt auch die Integration im Feld getrennt. Dies führt zu hohen Integrationskosten. Mit dem Einsatz der SAFETYLON-Technologie werden alle Geräte – ob sicher oder nicht sicher – in der gleichen Art und Weise gebunden und kommissioniert. Dafür können herkömmliche, bereits am Markt verfügbare LNS®-Tools verwendet werden (ab LNS 3.2x bzw. LNS Turbo). LNS-Plug-Ins stehen zur Verfügung, um die sicheren Geräte mit einer sicheren Konfiguration zu versehen (Abbildung 7). Bei Bedarf können diese Plug-Ins applikationsspezifisch angepasst werden. Darüber hinaus sind keine weiteren Tools für die Inbetriebnahme erforderlich.

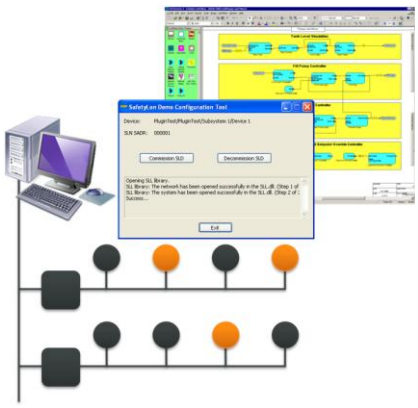

Abbildung 7: Inbetriebnahme mit Standard-Tools und Plug-Ins

Für sichere Anwendungen sind generell sorgfältige Tests der Anlagen vorgeschrieben. Beim Einsatz der SAFETYLON-Technologie ergibt sich jedoch der Vorteil, dass keine zusätzlichen Tools verwendet werden müssen, sondern dass hierfür LNS-Plug-Ins zur Verfügung stehen. Darüber hinaus ist es möglich, die Tests der sicheren Funktionen in die normalen Tests einer LON-Anlage zu integrieren. Beides führt zu geringeren Aufwendungen während des Integrationsprozesses.

Sichere Geräte

Während mit herkömmlicher Technik bei hohem Aufwand maximal SIL 2-Anwendungen realisiert werden können, ist mit der SAFETYLON-Technologie erstmals die wirtschaftliche Umsetzung von sicheren Anwendungen in LON-Netzwerken für SIL 3 möglich. Dazu ist in den Geräten ein hoher Diagnosedeckungsgrad erforderlich. Die Hard- und Softwarearchitektur ist daher so ausgelegt, dass diese hohen Anforderungen erfüllt werden können. Dabei sind die eingesetzten Prozessoren flexibel auswählbar, so dass anwendungsabhängig passende, effektive und kostengünstige Designs erstellt werden können.

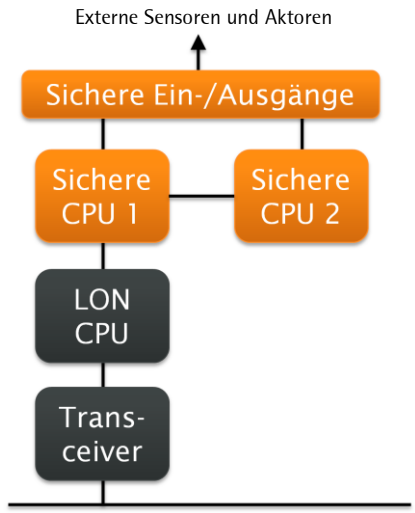

Abbildung 8: Hardware-Architektur eines SAFETYLON-Knotens

Die Hardware (Abbildung 8) besteht aus einer LON-CPU mit entsprechendem Transceiver und einem Sicherheitskern. LON-CPU und Transceiver gehören zu dem sogenannten „Black Channel“, welcher nicht sicherheitsrelevant ist. Die Sicherheit wird innerhalb des Sicherheitskerns durch zwei

sichere CPUs mit entsprechender Ein- und Ausgangsbeschaltung erzeugt. Unterstützt werden alle drahtgebundenen Medien.

Zurzeit werden LON-CPUs von Echelon® und LOYTEC unterstützt. Andere LON-CPUs können während der Produktentwicklung integriert werden. Sichere CPUs können aus der ARM®-Familie oder frei gewählt werden.

Sichere Firmware

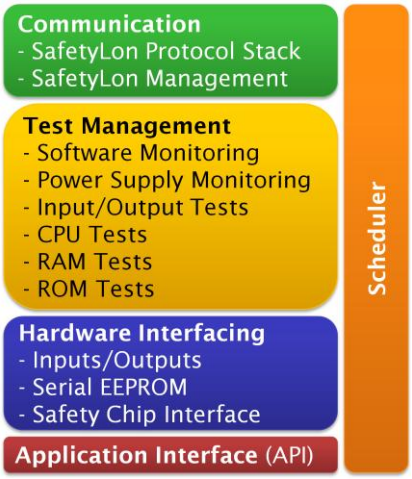

Abbildung 9: Software-Architektur eines SAFETYLON-Knotens

Die sichere Firmware (Abbildung 9) verfügt über ein einfaches Betriebssystem (Scheduler-Prinzip). Die Kommunikationsschicht behandelt sowohl das SAFETYLON-Protokoll als auch die zugehörigen Netzwerkmanagement-Dienste. Für die Sicherheit ist ein umfangreiches Testmanagement erforderlich und entsprechende Treiber ermöglichen den Zugriff auf die Hardware. Die sichere und produktspezifische Applikation wird über ein API (Application Program Interface) eingebunden.

Entwicklungsergebnisse

Zurzeit stehen folgende Ergebnisse für eigene Produktentwicklungen zur Verfügung:

- Sicherheitskonzept für die SAFETYLON-Technologie inklusive Beurteilung des TÜV Rheinland für Anwendungen bis SIL 3 nach IEC 61508.
- Hardware: Spezifikationen, Schaltpläne, Leiterplattenlayouts, Stücklisten, Produktionsdaten, FMEA-Berechnungen für Referenz-Design
- Software: Spezifikationen, Quellcode Firmware, Quellcode Applikationsbeispiele für Referenzdesign
- Entwicklungs-Tools: Spezifikationen, Quellcode Shortstack/Orion Stack Client, SAFETYLON LonMark Device Resource Files, Quellcode SAFETYLON Application Builder, Installationsskripts
- Netzwerkmanagement-Tools: Spezifikationen, Quellcode für SAFETYLON PC Library, Quellcode für SAFETYLON Plug-In Application, Installationsskripte
- Testumgebung: Spezifikationen, SAFETYLON Test Suite, Quellcode für Test Suite und weitere Testsoftware
- Beurteilung der Ergebnisse durch den TÜV Rheinland.

Abbildung 10: SAFETYLON-Referenzdesign auf Basis des L-Chip® (LOYTEC)

Darüber hinaus steht das Referenzdesign in Form von mehreren Baugruppen zur Verfügung. Das Referenzdesign kann gleichzeitig als Entwicklungsplattform verwendet werden.

Produktentwicklung

Hersteller können die SAFETYLON-Entwicklungsergebnisse für Ihre eigenen Produktentwicklungen nutzen. Während der Entwicklung sollten die Vorgaben der IEC 61508 bezüglich des Lebenszykluskonzeptes beachtet werden.

Dieses setzt ein applikationsspezifisches Sicherheitskonzept voraus, welches insbesondere die Zielanwendung des Produktes mit den anzuwendenden Normen und Richtlinien beschreibt. Bei der Erstellung dieser Spezifikation (Safety Requirement Specification) können große Teile des SAFETYLON-Konzeptes referenziert werden, so dass der Aufwand dieser Spezifikation begrenzt bleibt. Es wird empfohlen, das Sicherheitskonzept frühzeitig zu erstellen und eine positive Beurteilung durch eine Prüfstelle (z.B. TÜV) anzustreben.

Anschließend kann der Entwicklungsprozess gestartet werden. Dieser setzt ein Management der funktionalen Sicherheit[3] voraus, um systematische Fehler während der Entwicklung möglichst zu verhindern. Weitere Anforderungen der anzuwendenden Standards sollten für die Hard- und Softwareentwicklung selbstverständlich beachtet werden.

Am Ende der Entwicklung steht die Zulassung des Produktes oder Systems im Rahmen einer Baumusterprüfung durch eine Prüfstelle und die Überführung in die Produktion und den Vertrieb.

Fazit

Mit der SAFETYLON-Technologie steht dem Markt eine leistungsfähige Lösung zur Verfügung, mit der sichere Anwendungen bis SIL 3 in existierenden oder neuen Projekten wirtschaftlich realisiert werden können. Hersteller greifen dabei auf Ergebnisse zu, die sowohl die Hardware, embedded Software, Entwicklungstools, Inbetriebnahme-Tools und Testumgebungen einschließt.

Weitere Informationen stellt der LONMARK Deutschland e.V. auf Anforderung gerne zur Verfügung.

[3] Auch ‚Funtional Safety Management' oder ‚FSM'. Dient der Qualitätssicherung während des gesamten Sicherheitslebenszyklus.

Über LON

Die LON Technologie – mit ANSI/CEA-709.x und CEA-852 standardisiert sowie als EN14908 in das europäische und als ISO/IEC14908 in das internationale Normenwerk übernommen – ermöglicht den neutralen Informationsaustausch zwischen Anlagen und Geräten von verschiedensten Herstellern und unabhängig von den Anwendungen. Die LON Technologie ermöglicht somit eine einheitliche Betrachtung der unterschiedlichsten Anwendungen und das Ausnutzen von Synergieeffekten zwischen diesen.

Über den Autor

Martin Mentzel beschäftigt sich mit der LON-Technologie seit 1995 und mit der funktionalen Sicherheit seit 2003. Er ist Functional Safety Engineer (TÜV Rheinland), Inhaber der Mentzel GmbH, geschäftsführender Gesellschafter der SafeSquare GmbH, seit 2008 Mitglied des Vorstandes des LONMARK Deutschland e.V. und hat die SAFETYLON-Entwicklung als technischer Projektkoordinator begleitet.

Martin Mentzel ist erreichbar unter SafeSquare GmbH, Max-Planck-Straße 1, 42477 Radevormwald, Tel.: 02195–8038753, Fax: 02195–8038754, E-Mail martin.mentzel@safesquare.eu.

Über LONMARK Deutschland e.V.

LONMARK Deutschland e.V. versteht sich als Interessenvereinigung aller Anwender und Entwickler rund um LON im deutschsprachigen Raum. Ziele sind die Durchsetzung der LON Technologie in der Automatisierungs-, Gebäude-, Gastronomie-, Prozess- und Umwelttechnik, der Informationsaustausch über Produkte und Entwicklungen, gemeinsames Marketing und Interessenvertretung in Politik und Verbänden. LONMARK Deutschland e.V. ist aus der 1993 gegründeten LON Nutzer Organisation e.V. (LNO) hervorgegangen, die 2006 ihren Namen in LONMARK Deutschland e.V. geändert hat. LONMARK Deutschland e.V. zählt zurzeit rund 90 Mitglieder, wovon jeweils ein Viertel auf Großkonzerne, Mittelständler, Ingenieurbüros und Forschungsinstitute entfällt.

Weitere Informationen erhalten Sie bei LONMARK Deutschland e.V., Theaterstr. 74, 52062 Aachen, Tel.: 0241–88970–36, Fax: 0241–88970–42, E-Mail office@lonmark.de, www.lonmark.de.