

SAFETYLON – ein innovatives Konzept für sicherheitsgerichtete Anwendungen in der Gebäudeautomation

Dr. Jürgen W. Hertel, Consortium Manager des Collective Research Projects SAFETYLON (012611) im 6. Rahmenprogramm der Europäischen Kommission (CR6), stellt im Folgenden das innovative SAFETYLON Konzept vor. SAFETYLON macht die Eigenschaften und Vorteile von LON für sicherheitsgerichtete Anwendungen in der Gebäudeautomation nutzbar.

Im Rahmen des 6. Framework Program for Collective Research hat die Europäische Kommission im Januar 2005 ein F&E Projekt „SAFETYLON“ an ein Konsortium von Firmen und Universitäten vergeben, die langjährige Erfahrung mit der Entwicklung und Vermarktung der offenen Netzwerktechnologie LON mitbringen. Nur ein Mitglied hatte auch umfangreiches Wissen und langjährige Erfahrung mit Sicherheitstechnologie. Herz der LON Technologie ist ein Kommunikationsprotokoll, auch bekannt als ANSI 709 oder EN 14908 Standard. LON wird vorwiegend in Anwendungen der Gebäudeautomation eingesetzt, von kleinen bis hin zu sehr großen Bürogebäuden, aber auch in vielen anderen Gebieten in der Industrie, im Verkehrswesen und sogar in Wohngebäuden.

Ende der 90er Jahre wurde international ein allgemeiner Standard für Sicherheit entwickelt, bekannt unter der Bezeichnung

IEC 61508. Er betrifft alle technischen Systeme, die Menschen, die Umwelt oder materielle Güter gefährden. Da moderne Steuerungssysteme auf Kommunikationsprotokollen, Verarbeitung von Ein- und Ausgangssignalen und vielen elektronischen Komponenten basieren, betrifft die Sicherheitsnorm IEC 61508 das gesamte Sicherheits-Netzwerk. Beispiele sind großflächige, gefährliche Situationen wie Feuer, ausströmendes Gas oder Erdbeben. Solche Ereignisse müssen mit einer sehr hohen Wahrscheinlichkeit erkannt werden, um danach einen bestimmten sicheren Zustand oder ein sicheres Szenario einzuleiten.

Alle bekannten seriellen Kommunikationsprotokolle sind weit davon entfernt, eine „Restwahrscheinlichkeit der Fehlererkennung“ zu gewährleisten, die der Sicherheitsstandard verlangt. Um den IEC 61508 Safety Integrity Level 3 (SIL 3) zu erfüllen, musste SAFETYLON daher als ein „Protokoll im Protokoll“ entwickelt werden, zusammen mit der dazugehörigen Hard- und Software.

Dieser Artikel soll Ihnen das Konzept des IEC 61508 Sicherheitsstandards und die Merkmale von SAFETYLON nahe bringen. Nach einigen Grundsätzen über Sicherheit wird erklärt, wie das SAFETYLON Projekt organisiert und aufgeteilt ist und wie die sicheren Hard- und Software-Module spezifiziert, aufgebaut, getestet und eingesetzt werden.

Zum Schluss wird noch aufgezeigt wie die neue Technologie umgesetzt werden soll.

1. Motivation

In unserer heutigen Welt werden mehr und mehr Funktionen in Industrieautomation, Fertigungssteuerung und Gebäudeautomation von vernetzten Steuerungen und Geräten bewältigt. Auf der anderen Seite beinhalten mehr und mehr dieser Funktionen Gefahren für Gesundheit, Leistungsfähigkeit und Überlebenschancen für Personen im Umfeld von potenziell gefährlichen Maschinen, Anlagen oder technischen Ausrüstungen. Diese Funktionen werden Sicherheitsfunktionen genannt. Sie sind in den sieben Bänden des IEC 61508 Standards umfassend analysiert und beschrieben. Sicherheit bezieht sich nicht nur auf ein Produkt oder ein Netzwerk von zusammenwirkenden Produkten. Sie deckt auch die gesamte Lebensdauer eines Produktes ab, von der Entwicklung bis zum Einsatz und letztendlich bis zur Entsorgung eines Produktes oder Systems. Weiterhin beinhaltet sie alle Maßnahmen und Bedingungen, die eine Person oder ein Unternehmen beim Umgang mit Sicherheit beachten muss – bei der Entwicklung, Herstellung und Installation eines sicheren Produktes oder eines sicheren Systems. Dies nennt man funktionales Sicherheitsmanagement (FSM), welches eine wichtige Rolle spielt, wenn ein

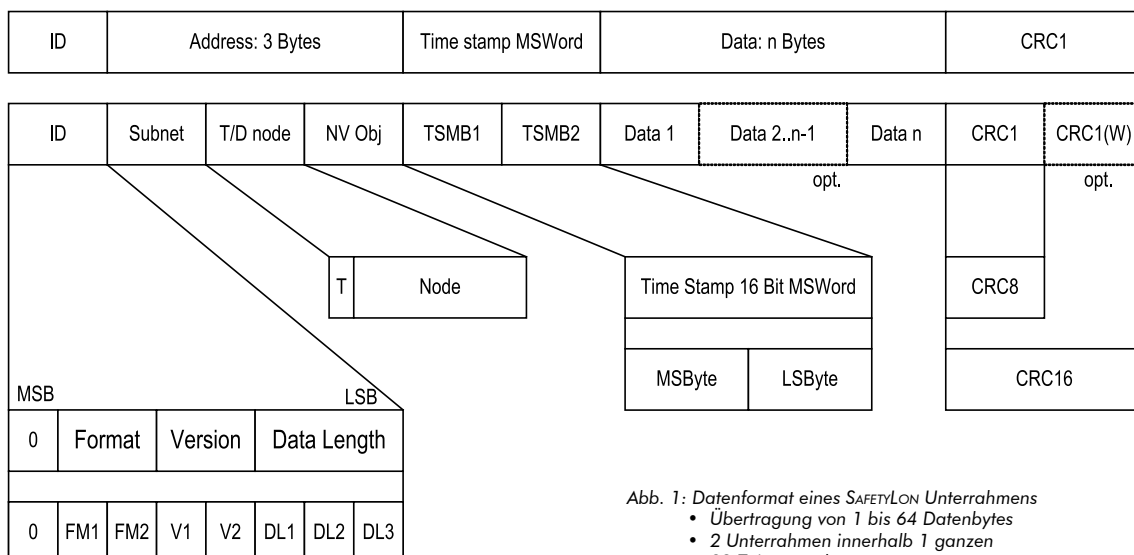


Abb. 1: Datenformat eines SAFETYLON Unterrahmens

- Übertragung von 1 bis 64 Datenbytes
- 2 Unterrahmen innerhalb 1 ganzen
- 32 Zeitstempel
- Variable CRC (8 oder 16 Bits)

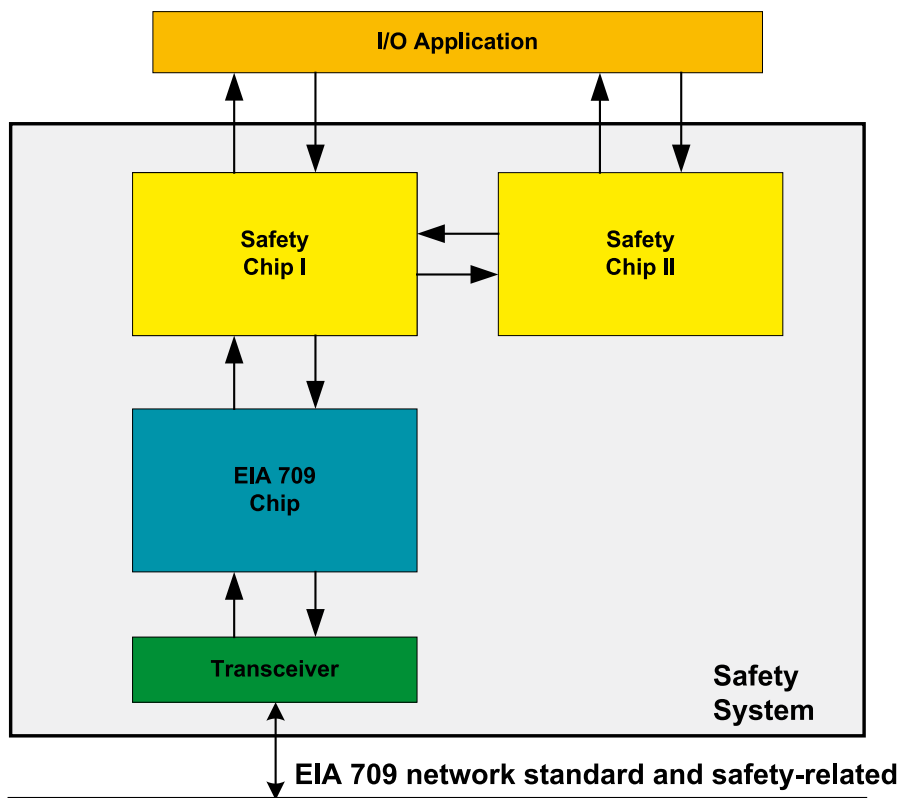


Abb. 2: SAFETYLON 1oo2 Architektur: Ein einzelner Kommunikationschip und zwei identische Safety Chips

autorisiertes Gremium wie der deutsche TÜV damit beauftragt wird, ein sicheres Produkt zu bewerten und zu zertifizieren, bevor es im Markt eingeführt wird.

Im Bereich der Gebäudeautomation gibt es eine ganze Reihe von Funktionen, die eine Safety Integrity Level (SIL) Einstufung unbedingt erfordern: Beispiele sind Aufzugsteuerungen, Fluchtwegauszeichnung, Feuer- und Rauchmeldung, automatische Brandbekämpfung durch Lüftungskontrolle, Sprinkleranlagen und Feuerschutztüren, Notbeleuchtung, Notausgänge – um nur die Wichtigsten zu nennen.

Im Jahre 2003 wurde vom Vorstand der damaligen LNO eine Arbeitsgruppe „Sicherheit“ ins Leben gerufen, um dieses Thema zu analysieren und den Versuch zu starten, ein neues „SAFETYLON“ Protokoll in Verbindung mit einer „zweikanaligen“ Hardware-Architektur aufzusetzen, das die Anforderungen des IEC 61508 Standards erfüllt. Die Gruppe suchte professionelle Unterstützung bei einem erfahrenen Berater (Dr. Peter Wratil von innotec). Dr. Wratil wurde vom LNO Vorstand beauftragt, die Arbeitsgruppe zu leiten und sie dabei zu unterstützen, eine Machbarkeitsstudie zu erstellen. Diese wurde später vom TÜV Rheinland bewertet und akzeptiert (Prinzippapier). Leider – oder im Nachhinein

betrachtet, glücklicherweise – schlugen alle Versuche fehl, eine eigenständige Finanzierung zur Entwicklung einer sicheren LON Lösung durch interessierte LNO Mitglieder auf die Beine zu stellen. Daher entschloss sich die Gruppe, sich um eine Förderung aus dem 6. Rahmenprogramm der EU für konsortiale Forschungsprojekte (Collective Research) zu bewerben und war damit erfolgreich. Der Vertrag wurde schließlich im September 2005 unterzeichnet.

2. Das SAFETYLON EU Projekt

Ziel des SAFETYLON Projektes ist die Erstellung einer universellen, offenen Lösung, die die Prinzipien von LON- und LONMARK-Netzwerken so weit wie möglich verwendet, um eine offene Kommunikationslösung zu schaffen, die die IEC 61508 Norm erfüllt. Genauer gesagt: Es werden die gesamte LON Infrastruktur wie das LON (oder EIA 709 oder EN 14908) Protokoll, alle physikalischen Medien nach LONMARK, sowie Router, Repeater und Standard LONMARK Knoten in einem Netzwerk ohne Änderung beibehalten, sogar IP Router und das EIA 852/IP Tunneling Protokoll. Dies bedeutet, dass in einem normalen LON Netzwerk nicht sichere und sichere Kommunikation nicht nur koexistieren können, sondern dass beide „Teilnetzwerke“ die gleiche Netzwerkinfrastruktur nutzen und sogar intern Daten

austauschen können. Wie man es von einer offenen Sicherheitslösung erwarten kann, werden gleich zwei Implementierungen basierend auf dem FT3120 Smart Transceiver von Echelon und dem LC3020 (Lisa) Prozessor von Loytec parallel entwickelt und können später sogar im Feld ausgetauscht oder aufgerüstet werden.

Zweites Ziel, speziell aus Sicht der EU, ist die Einbindung mehrerer Nutzerorganisationen und Firmen aus mehreren Ländern in das Projekt. Ein ausgewogenes Konsortium zusammenzustellen, um die vielen unterschiedlichen Aufgaben auszuführen, die nötig sind, um die vorgegebenen Ziele und Ergebnisse zu erreichen, war die größte Herausforderung. Es gibt drei unterschiedliche Gruppen, die wohl definierte Aufgaben zu erfüllen haben:

1. Die Research and Technology Development (RTD) Gruppe, bestehend aus drei Universitäten (TU Wien, FH Dortmund, AGH-UST Krakau) und drei industriellen Entwicklern (Loytec, who Ingenieurgesellschaft, innotec).
2. Die Gruppe der Small and Medium Enterprises (SME), die sich aus sieben relativ kleinen Firmen mit LON Erfahrung zusammensetzt: APICE (Italien), IBT (Schweiz), Intron Engineering und UNITRO Fleischmann (Deutschland), Newron System (Frankreich), Naronic (Schweden) und Zdanica (Polen).
3. Die Industrial Association Gruppierung (IAG) mit LONMARK Deutschland e.V. als Konsortialführer sowie LONMARK Schweden und der Polnischen LON User Group (PLUG).

Die Idee hinter dem Zusammenspiel der drei Gruppen ist so einfach wie effektiv: Die RTDs designen und entwickeln eine neue Technologie, und die SMEs bauen darauf auf mit Prototyp-Anwendungen und sicheren Prototyp-Produkten. Auf der anderen Seite kümmern sich die IAGs um die Absicherung des geistigen Eigentums durch Patentierung – ein Patent wurde am 23. April 2007 unter der Patent-Nr. 07008251.6-1244 vom LONMARK Deutschland e.V. beim Europäischen Patentamt in München angemeldet – der innovativen Bestandteile der Erfindung (exploitation alias Verwertung), sowie durch Lizenzierung des geistigen Eigentums und der Bestandteile der Technologie, Verbreitung des Wissens auf Konferenzen sowie in Seminaren, Workshops und Veröffentlichungen (dissemination alias Vermarktung). Darüber hinaus sind die IAGs verantwortlich für die Entwicklung und Durchführung von Schulungen, jede in ihrem Territorium.

LONMARK Schweden ist zuständig für alle skandinavischen Länder sowie Großbritannien und Irland, PLUG für alle osteuropäischen Länder und Russland und LONMARK Deutschland für das kontinentale West-, Mittel- und Südeuropa.

Das Projekt läuft über einen Zeitraum von 36 Monaten und ist mit ca. 3 Mio. € dotiert, wovon ca. 1 Mio. von den 16 Mitgliedern kofinanziert werden muss. Auch wenn dies viel erscheint – für eine geografisch verteilte organisierte Hard- und Softwareentwicklung sowie weitere Aufgaben zur Sicherung des geistigen Eigentums (IPR) und der Vermarktung der Ergebnisse, die ja alle geplant und zu Ende geführt werden müssen, ist es das nicht. Trotz der Nutzung moderner, webbasierter Kommunikations- und Dokumentationssysteme wie Projektplace wird ein nicht unbedeutender Anteil für Reisekosten und Koordination verbraucht.

Das Projekt ist in acht Arbeitspakete aufgeteilt, die alle von unterschiedlichen Partnern ausgeführt werden (die Verantwortlichen sind in Klammern genannt):

1. Definition der Anforderungen, Spezifikationen, Qualitätssicherung für sichere Komponenten und das gesamte System (innotec)
2. Entwicklung der Sicherheitssoftware (Safety Operating Software oder SOS) die auf der sicheren Hardware-Entwicklungsplattform (4) läuft (ICT Wien)
3. Entwicklung von Tools zur Entwicklung sicherer und interoperabler Knoten und deren Installation und Inbetriebnahme in einer sicheren Prozedur (FH Dortmund)
4. Erstellung einer sicheren Hardware-Entwicklungsplattform bestehend aus zwei

steckbaren, sicheren Kernmodulen mit FT3120 oder LC3020 als Kommunikationsprozessoren, einer sicheren Hauptplatine mit vielen Schnittstellen zum Bau von Prototypen sowie einer digitalen I/O Karte (Loytec)

5. Entwicklung von acht sicheren Prototyp- und Demonstrator-Anwendungen (IBT)
6. Verwertung und Vermarktung der RTD Ergebnisse (LONMARK Deutschland)
7. Training (AGH-UST)
8. Projekt Management (LONMARK Deutschland)

Alle Arbeitspakete setzen sich aus Unterpaketen zusammen, die sorgfältig geplant, überwacht und aktualisiert werden müssen. Aufgrund maßgeblicher Änderungen der Hardwarearchitektur des Kern-Sicherheitsmoduls (siehe Abschnitt 4) haben sich die Arbeitspakete (4) und (2) um Monate verzögert. Im Ergebnis hat dies aber trotzdem einen positiven Effekt: eine weitgehend symmetrische und daher sehr robuste und gut wartbare Hard- und Software-Lösung für SAFETYLON.

Das SAFETYLON Projekt befindet sich jetzt in seinem dritten Jahr und ist gut im Plan. Hard- und Software sind fast fertig gestellt und werden zurzeit durch die Ingenieure von AGH-UST und innotec in einer wohl durchdachten Testumgebung auf Herz und Nieren überprüft. Gleichzeitig entwickeln und testen Loytec, who, IBT und die anderen SMEs ihre ersten Prototypanwendungen. Und während sich das Projekt seinem Ende nähert, stellt innotec alle Dokumente zusammen, die im Laufe des Projekts erstellt wurden und überprüft sie, mit dem Ziel, die Zulassung/Zertifizierung der beiden Kern-Sicherheitsmodule und ihrer Sicher-

heits-Betriebssoftware (SOS) durch den TÜV Rheinland zu erreichen.

Die folgenden Abschnitte enthalten das Wesentliche der SAFETYLON Lösung. Eine vollständige und detailliertere Beschreibung wird zu einem späteren Zeitpunkt in einem technischen Dokument (white paper) veröffentlicht.

3. SAFETYLON Protokoll

Das SAFETYLON Protokoll profitiert von der Tatsache, dass das EIA 709 oder EN14908 Protokoll über eine variable Datenlänge von bis zu 228 Bytes verfügt. So kann man ein Protokoll auf der Applikationsschicht oder einfach gesagt ein „Protokoll im Protokoll“ definieren. Es ist seit langem bekannt, dass die Anforderungen des IEC 61508 nur erfüllt werden können, wenn die sicheren Daten zweimal erzeugt und übermittelt werden, um danach Bit für Bit auf der Empfangsseite verglichen zu werden. Nur so kann die so genannte „durchschnittliche Fehlerwahrscheinlichkeit pro Ereignis (bei hoher Last oder im kontinuierlichen Betrieb) kleiner als 10^{-9} gehalten werden. Dies entspricht dem höchsten Safety Integrity Level SIL3 (die Restfehlerwahrscheinlichkeit des Netzwerkes sollte nur 1% der Gesamtwahrscheinlichkeit von 10^{-7} pro Stunde betragen). Daher besteht ein SAFETYLON Protokollrahmen aus zwei identischen Unterrahmen, wovon nur einer dargestellt ist (s. Abb. 1).

Jeder Unterrahmen kann bis 64 Datenbytes enthalten. Dabei wurde die Datenlänge eines jeden Datums bewusst auf 5 Datenlängen (0, 1, 2, 4 und 8) beschränkt, da größere Datenlängen (z. B. Textnach-



Abb. 3: SAFETYLON Kernmodul basierend auf dem LC3020 Chip (Lisa) von Loytec

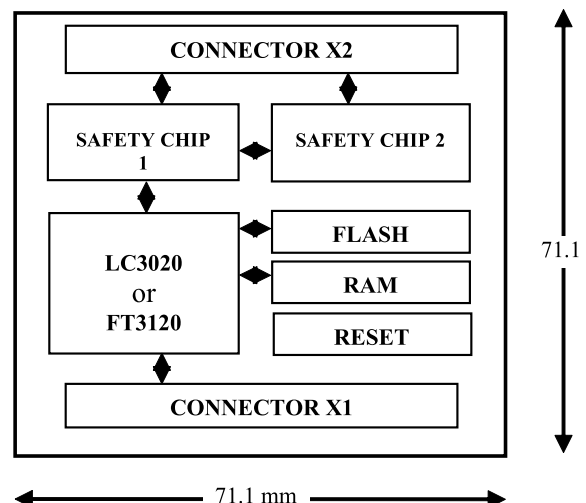


Abb. 4: Hauptkomponenten der zwei verfügbaren SAFETYLON Kernmodule von Loytec (LC3020 basiert) oder who Ingenieurgesellschaft (Neuron FT3120 basiert)

Sonderdruck

richten) in Sicherheitsanwendungen nicht sinnvoll sind. Da für die Zieladressierung der domainweite Broadcast von Standard LON verwendet wird, der gleichzeitig alle Netzwerkteilnehmer erreicht, braucht ein SAFETYLON Rahmen nur noch eine sichere Quelladresse. Jeder empfangende Knoten verfügt über eine Liste von Quelladressen, auf die er hört und anspricht. Die gesamte Nachricht wird nur dann weiterbearbeitet, wenn in beiden Safety Chips eine Übereinstimmung der Adressen festgestellt wird. Die Quelladresse enthält auch eine sichere, ein Byte lange NV ID, die abweichend von Standard LON explizit übermittelt wird. Bei allen relevanten LONMARK SNVTs, die der erwähnten Datenlängenbeschränkung entsprechen, werden identische LONMARK IDs benutzt. Darüber hinaus und ebenfalls abweichend von Standard LON, enthält jede Nachricht einen Zeitstempel, der zur Synchronisation der Uhren des sendenden und empfangenden Knotens genutzt wird. Damit lassen sich dann kritische Verzögerungen, die einen vordefinierten maximal tolerierbaren Wert überschreiten, feststellen und sicherheitstechnisch nutzen. Die Synchronisation wird, abhängig von Überlegungen zu Systemdesign und Systemleistung, entweder von einem zentralen Zeitgeber (clock) oder dynamisch als Handshake zwischen jedem Sender-Empfänger Paar ausgeführt. Schließlich enthält jeder Unterrahmen zusätzliche unterschiedliche CRC Informationen, die, abhängig von der Länge des Unterrahmens, 8 Bit oder 16 Bit lang sein können, sodass ein minimaler Hammingabstand von 4 gewährleistet ist.

Um das oben Geschilderte richtig einschätzen zu können, ist es wichtig, sich

vor Augen zu halten, dass alle Informationen in den Unterrahmen nichts mit den Protokolldiensten der Ebenen 1 bis 6 des Standard LON Protokolls zu tun haben. Diese Protokolldienste werden häufig als „grauer“ Transportkanal bezeichnet, der nur genutzt wird, um auf transparente Weise die sicheren Rahmen von A nach B zu tunneln, ohne sich um deren Inhalt zu kümmern. SAFETYLON repliziert jedoch die meisten Dienste der Ebenen 1 bis 6 oder fügt sogar neue Dienste hinzu, wie zum Beispiel die Zeitstempelsynchronisierung. Diese Replizierung von Diensten ist übrigens einer der Ansprüche des SAFETYLON Patents.

Der Datenfluss einer sicheren Nachricht wird so abgewickelt, dass der Safety Chip #1 (s. Abb. 2) den Gesamtrahmen in zwei Unterrahmen unterteilt, den ersten Unterrahmen verarbeitet und den zweiten Unterrahmen zur Verarbeitung an den Safety Chip #2 übergibt. Der Inhalt beider Rahmen wird dann Bit für Bit über das serielle Interprocessor Interface (SCI) verglichen. Wenn identisch, werden die eingebetteten Daten zur weiteren Verarbeitung „freigegeben“, zum Beispiel um einen sicheren Ausgang zu schalten.

Umgekehrt wird ein Datum von einem physikalischen Eingang zunächst auf beide Safety Chips #1 und #2 verzweigt. Anschließend wird in jedem Safety Chip unabhängig voneinander je ein Unterrahmen gebildet und Bit für Bit über SCI verglichen. Nur wenn beide identisch sind, baut der Safety Chip #1 einen kompletten Rahmen, bestehend aus zwei identischen Unterrahmen, zur Übergabe an das Netzwerk auf.

4. SAFETYLON Hardware

Die SAFETYLON Hardware verwendet eine so genannte 1oo2 (lies: one out of two) Struktur, bestehend aus einem EIA 709 Chip als Standard LON Kommunikationsprozessor und zwei Safety Chips (s. Abb. 2)

Die Grundüberlegungen zur Entwicklung sicherer Hardware sind einfach. Für jedes Datum, das sicher zwischen einem Sender (producer) und einem Empfänger (consumer) übermittelt werden soll, müssen zwei, vorzugsweise diversitäre „Kanäle“ für Kommunikation und Verarbeitung vorhanden sein. Diese Anforderung betrifft alle an der Kommunikation beteiligten Elemente: das serielle Kommunikationsprotokoll, den physikalischen Ein- oder Ausgang von Daten, die Verarbeitungseinheit einschließlich Speicher und insbesondere die Steuerung der so genannten „sicheren Einheit im Fehlerfall“ (fail safe unit), einer Aktoreinheit, angesteuert von zwei unabhängigen Ausgangssignalen im Falle des Auftretens einer vordefinierten Fehlfunktion oder eines zufällig aufgetretenen Fehlers.

Alle Sicherheitsmerkmale, die unabhängig von irgendeiner speziellen Applikationshardware sind, werden in einem kompakten SAFETYLON Kernmodul zusammengefasst, das in die zugehörige Anwendungsbaugruppe gesteckt wird (s. Abb. 3 und 4). Diese besteht normalerweise aus zwei unabhängigen Stromversorgungen, einem Quarz und einer Anzahl digitaler I/O Punkte, die dupliziert und getrennt auf die entsprechenden Anschlussstifte des Kernmoduls geführt werden. Zur sicheren Überwachung der Stromversorgungen sind sichere analoge Eingänge implementiert. Analogausgänge oder ein serielles Protokoll über digitale I/O-Kanäle sind eher untypisch für sicherheitsgerichtete Anwendungen und wurden daher in diesem Projekt nicht berücksichtigt. Im Prinzip werden alle LON Medien, auch Powerline, unterstützt, obwohl nur die für die Gebäudeautomation wichtigen Free Topology und EIA852/IP Kanäle innerhalb des Projektes implementiert werden.

Sichere I/O-Hardware muss permanent auf ihre Integrität getestet werden, um sicher zu stellen, dass die Hardware zum Zeitpunkt des Empfangs oder der Übermittlung einer sicheren Nachricht oder eines sicheren Ein- oder Ausganges korrekt arbeitet. Eine sehr effiziente Methode dazu ist ein wechselseitiger Check beider Safety Chips durch Senden und Empfangen von CPU-generierten Testimpulsen und deren „Durchlaufen“ aller Schaltkreise der Applikationsbaugruppe. In

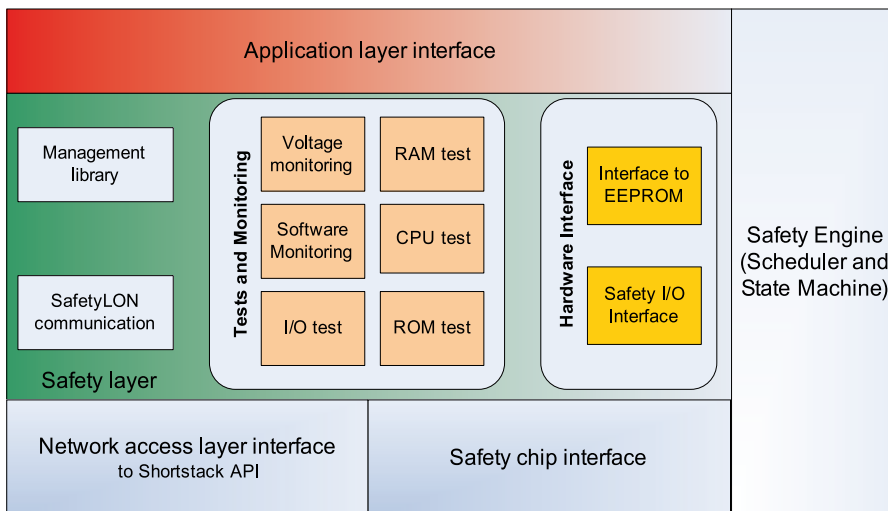


Abb. 5: Die Architektur der Safety Operating Software (SOS) die auf dem Safety Chip #1 läuft. Im Safety Chip #2 wird das Netzwerkzugriffs-Layerinterface nicht benötigt.

Abb. 5 ist der Hardware I/O-Integritätstests – mit I/O bezeichnet – nur einer von sechs Typen solcher Tests. Die Testimpulsmethode verhindert, dass das Wissen über den inneren Zustand der Hardware mit der Zeit an Aktualität verliert, was dazu führt, dass das System immer mehr an Sicherheit verliert.

Für Softwareentwicklung, Prototypenerstellung und Testen haben Loytec und who eine voll ausgestattete Hauptplatine mit vier sicheren digitalen Eingängen und zwei sicheren digitalen Ausgängen, verbunden über mehrere Flachbandkabel, entwickelt, dazu zwei Stromversorgungen, zwei JTAG Schnittstellen, Platz für FT, PL und RS485 Transceiver sowie einen Bereich für Prototyping.

Heute sind alle RTDs und SMEs mit einem solchen Entwicklungskit ausgestattet. Es ist die Basis für die Entwicklung von acht Prototypen in den folgenden Anwendungsbereichen: Notbeleuchtung (IBT), Notstop im Aufzug (Intron Engineering), Fluchtwegauszeichnung (IBT), Alarmauslösung im Brand- und Einbruchfall (ZDANIA), Not-schalter am Ausgang einer Sicherheitstür (Naronic), Zugangskontrolle mit Sicherheitsfunktion (Apice), sichere Störanzeige- und Schalteinheit (Unitro Fleischmann) und ein sicheres Netzwerkmanagement Tool (Newron System).

5. SAFETYLON Software

Die SAFETYLON Software ist das Gehirn der SAFETYLON Lösung und bei weitem die komplexeste Entwicklung innerhalb des Projekts. Wie die Hardware, so muss auch die Software permanent ihre eigenen Hardwareresourcen wie Versorgung (Spannungspegel), CPU, RAM, ROM und I/O überwachen und sich dabei auch noch selbst testen. Daher findet man keine kommerzielle Software, die diese Aufgabe ausreichend effizient und sicher erledigen würde, ohne ungewünschten Verlust von CPU Zyklen und Leistung. Aus diesem Grunde hat das Konsortium den Weg gewählt, die gesamte Software von Grund auf neu zu planen und zu entwickeln. Kernstücke der Safety Operating Software (SOS) (s. Abb. 5) sind ein sicheres Betriebssystem (Safety Engine), bestehend aus einer interruptgesteuerten Zeitintervall-Steuerung (Scheduler), verbunden mit einem Zustandsautomaten (State Machine). Im Wesentlichen übernimmt diese das Testen von Hard- und Software, was die meiste Zeit (mehr als 60%) in Anspruch nimmt. Regelmäßig wird in jedem Zyklus auch die Anwendung oder ein Teil davon, abhängig von Größe und benötigter Laufzeit, abgearbeitet.

Ebenfalls regelmäßig muss der Scheduler die Hardwareschnittstellen zum EEPROM Speicher, zu den I/Os und zu den beiden Safety Chips bedienen. Im Falle des Safety Chips #1 muss auch das Interface zum entsprechenden Kommunikationschip, Neuron oder Lisa, bedient werden. Es ist daher offensichtlich, dass die Software der beiden Safety Chips nicht einfach Schritt für Schritt synchron ablaufen kann, sondern dass die Synchronisation durch spezielle Ereignisse oder Interrupts, wie z. B. einem Bit für Bit Vergleich einer Nachricht, immer wieder erzwungen wird.

Ein weiterer Teil der SOS Software ist das Application Layer Interface (API). Es enthält alle Basisfunktionen, die eine sichere Anwendung aufrufen kann, um sichere Daten korrekt zu übergeben oder abzuholen. Mit der Zeit soll eine sichere Funktionsbibliothek erstellt werden, um damit Funktionen auf einem höheren Level oder logisch komplexe Funktionen für aufwändigere Safety-Anwendungen erstellen zu können.

Eine weitere Softwarekategorie wurde von der Fachhochschule Dortmund entwickelt. Sie betrifft die Erstellung sicherer SNVTs entsprechend den LONMARK Richtlinien sowie die Entwicklung von Installations- und Inbetriebnahmesoftware, in Zusammenarbeit mit who und Newron System. Die gute Nachricht für Systemintegratoren ist hier, dass in einem ersten Schritt ein sicherer Knoten mit Standard LNS Tools installiert wird, ergänzt durch spezielle Tools (zum Beispiel in Form von LNS Plug-In), um sichere Adressen und Parameter zuzuordnen und

in einer sicheren Konfigurationsdatenbank abzuspeichern. In einem zweiten Schritt folgt dann die sichere Überprüfung dieser Konfigurationsdaten. Damit ist die Installation des sicheren Knotens abgeschlossen. Hierzu sollte angemerkt werden, dass es sogar noch erforderlich ist, eine Liste der in Schritt 1 generierten und in Schritt 2 überprüften Konfigurationsdaten auszu-drucken, die entsprechend den IEC 61508 Anforderungen von einer geschulten und für Sicherheit autorisierten Person verglichen und abgezeichnet werden muss.

6. Verwertung und Verbreitung

Gemäß Vertrag mit der Europäischen Kommission ist das Konsortium verpflichtet, das Wissen und die Rechte an geistigem Eigentum (IPR – Intellectual Property Rights) aller im Projekt erzielten Entwicklungen zu sichern, unter anderem durch ein europäisches Patent (exploitation / Verwertung). Im Besonderen geht das IPR auf die teilnehmenden IAGs über, die mit der Aufgabe und der Verantwortung beauftragt sind, solches Wissen und IPR mit allen Mitteln zu verbreiten (dissemination / Vermarktung).

Im Herbst 2007 werden LONMARK Deutschland, LONMARK Schweden und PLUG eine Lizenzvereinbarung vorstellen und veröffentlichen. Diese definiert die Bestimmungen und Voraussetzungen, zu denen eine Einzelperson oder eine Firma in Europa die SAFETYLON Technologie einschließlich aller Inhalte eines SAFETYLON Starterkits lizenzieren kann. Es wäre verfrüht, hier weitere Einzelheiten zu beschreiben. Mit einer Aus-

Typ	Beschreibung	Preis (k€) LE	Preis (k€) ME	Preis (k€) SE
A	SAFETYLON Hardwareentwickler Lizenz, nur für interoperable Designs (enthält alles)	150,0	75,0	37,5
B	SAFETYLON Anwendungsentwickler Lizenz, (kein Kernmodul Design, keine Quellen, enthält die komplette Dokumentation)	20,0	10,0	5,0
C	SAFETYLON Hardwareentwickler Lizenz (für interoperable und/oder proprietäre Designs)	400,0	200,0	200,0
Definition der EC	Belegschaft: Umsatz: Bilanzsumme:	in mindestens einem Kriterium oberhalb ME	< 250 ≤ 50 Mio € ≤ 43 Mio €	< 50 ≤ 10 Mio € ≤ 10 Mio €

Abb. 6: Verschiedene Lizenztypen für unterschiedliche Bedürfnisse von Hardware OEMs und Anwendungsentwicklern

nahme, die off am meisten interessiert: der Preis. Da im Projekt schwerpunktmäßig die teilnehmenden klein- und mittelständischen Unternehmen (SMEs) gefördert werden sollen, gibt es für diese gegenüber den Großunternehmen (LEs) auch eine spezielle Preisgestaltung. Gemäß der Empfehlung, 2003/361/EC vom 6. Mai 2003 wird ein Unternehmen als klein (SE) eingestuft, wenn es eine Belegschaft von unter 50 und einen Umsatz von weniger oder gleich 10 Mio. € oder eine Bilanzsumme von weniger oder gleich 10 Mio. € hat. Es wird als mittleres Unternehmen (ME) eingestuft, wenn es eine Belegschaft von unter 250 und einen Umsatz von weniger oder gleich 50 Mio. € oder eine Bilanzsumme von weniger oder gleich 43 Mio. € hat. Wenn es nur bei einem Kriterium darüber liegt, ist es ein großes Unternehmen (LE). Die Preistabelle in Abb. 6 bezieht sich auf diese Definitionen.

Die Tabelle in Abb. 6 enthält drei Typen von Lizenzen. Typ A richtet sich an Produkt OEMs, die daran interessiert sind, ihre eigene SAFETYLON Hard- und Software zu entwickeln, aber gleichzeitig auch völlig interoperabel mit dem SAFETYLON Protokoll und der Installationsprozedur bleiben möchten. Typ B Lizenznehmer sind in erster Linie daran interessiert, ihre eigene I/O Hardware und Anwendungssoftware zu entwickeln, aber ein oder beide Kern-Sicherheitsmodule bei Loytec oder who zu kaufen. Der Vorteil ist, dass diese Kernmodule einschließlich der Safety Operating

Software (SOS) bereits eine Baumusterprüfung/Zertifizierung durch den TÜV Rheinland haben und die Zertifizierung eines fertigen Produktes basierend auf solch einem Kernmodul erheblich kostengünstiger ist. OEMs die sich – warum auch immer – entscheiden, die SAFETYLON Technologie auf proprietäre Art zu nutzen, können eine in diesem Sinne unlimitierte Kategorie C Lizenz erwerben.

Natürlich stellt sich in der Anfangsphase einer neuen Entwicklung immer die Frage nach Hilfe und Unterstützung. Ganz bewusst werden die drei Nutzerorganisationen diese Aufgabe Beratern und Dienstleistern überlassen. Im Laufe des Projekts haben sich insgesamt 13 Unternehmen, 3 Institutionen und viele Einzelpersonen detailliertes Wissen über Safety angeeignet und Erfahrungen mit SAFETYLON gesammelt; sie werden ihre Dienste dafür anbieten. Zu den weiteren Verwertungsaktivitäten gehört auch der Start einer SAFETYLON Website im 4. Quartal 2007. In Hinsicht auf den IEC 61508 Standard wird diese Website viel Wissenswertes enthalten, alle öffentlichen Termine wie SAFETYLON Seminare, Workshops und Schulungen ankündigen; aber auch einen geschützten Bereich für Lizenznehmer bieten, mit den aktuellen technischen Neuigkeiten und einer Download-Sektion für Updates.

7. Zusammenfassung und Ausblick

Das SAFETYLON Projekt ist eine bedeutende

Initiative von 16 europäischen Institutionen und Unternehmen, eine neue Technologie für sicherheitsgerichtete, interoperable Produkte und Anwendungen basierend auf Standard LON zu schaffen. Ohne die europäische Förderung für Collective Research im 6. Rahmenprogramm wäre es für jedes einzelne Unternehmen unmöglich gewesen, sich eine technisch so ausgereifte Lösung auszudenken, ganz zu schweigen vom Zugewinn an Wissen und Erfahrung mit dem Thema Sicherheit als neue Herausforderung für alle teilnehmenden Partner. In diesem Sinne gilt der Dank der Konsortiumsmitglieder auch allen Betreuern des Projekts in Brüssel, die uns mit Rat und Tat unterstützt haben und weiterhin unterstützen.

Nächster Schritt wird ab Oktober 2007 die Weitergabe dieses Wissens an die Mitglieder in der LONMARK Deutschland und den anderen Nutzerorganisationen sein – in Seminaren, Workshops und Schulungen. Es wird erwartet, dass jede IAG-Anwenderorganisation ein oder mehrere interessierte Unternehmen findet, bei denen die SAFETYLON Technologie auf Interesse stößt und die vom Abschluss einer Lizenzvereinbarung profitieren können, indem sie die Ergebnisse des SAFETYLON Projekts frühzeitig aufgreifen. Die Mitglieder des Konsortiums freuen sich darauf, dabei Hilfestellung zu leisten.



Dr. Jürgen W. Hertel • Consortium Coordinator SAFETYLON Project
D-85630 Grasbrunn • Tel. +49 89 456 55 91 • hertel@lonmark.de