Wie realisiert man vernetzte sicherheitskritische Systeme?

Ein systematischer Weg am Beispiel einer Antriebssteuerung

Markus Maier, Assystem Germany

Ob Analyse von Prozessdaten oder einfach nur die effiziente Umsetzung von Software Updates im Feld: Neue Geschäftsmodelle erfordern zunehmend die Öffnung einst abgeschotteter sicherheitskritischer Steuerungssysteme. Assystem zeigt einen systematischen Weg der Entwicklung sicherheitsbezogener vernetzter Systeme am Beispiel einer Antriebssteuerung unter Einhaltung der für den Anwendungsfall relevanten Security- & Safety-Standards.

In der Automatisierungstechnik vollzieht sich seit einigen Jahren ein Wandel hin zu modularen, vernetzten Systemen. Im Zuge dessen wird Cybersicherheit zur unabdingbaren Voraussetzung für funktional sicherheitskritische Systeme.

Erst Anfang des Jahres 2018 zeigte der Triton Malware Angriff auf eine Industrieanlage im Nahen Osten wie verwundbar aktuelle sicherheitskritische industrielle Steuerungssysteme sind.

Abbildung 1 zeigt unser Anwendungsbeispiel eines vernetzten E-Antrieb Controllers, der unter Anderem in Wasserkraftwerken und leistungsstarken Maschinen eingesetzt wird.

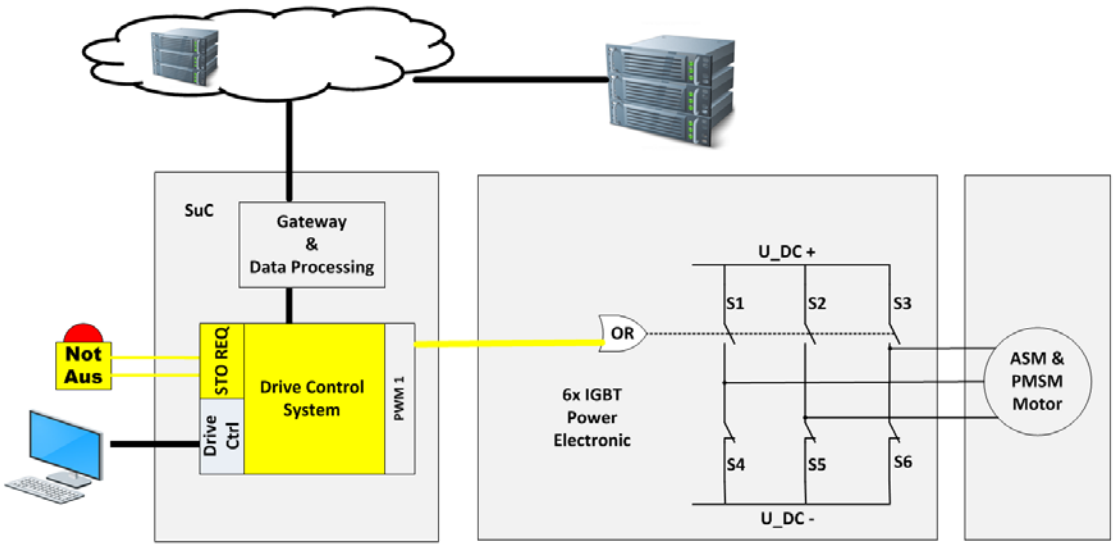

Figure 1 - Anwendungsbeispiel: vernetzter E-Antrieb Controller

Das zu betrachtende System (SuC) unseres Anwendungsbeispiels regelt die Steuerung eines E-Motors und ist mit einer Backend-/Cloud-Infrastruktur vernetzt. Dies ermöglicht einerseits die Überwachung des Steuerungsprozesses und andererseits auch Updates nicht funktional sicherheitsbezogener Software Anteile.

Die zentrale Safety Funktion für den Antrieb ist die sogenannte Safe Torque Off Funktion (STO), die in Bezug auf Cybersicherheit besonders geschützt werden muss. Weitere zu schützende Funktionen sind beispielsweise die E-Motor Regelung, der Maschinenstatus, die Diagnose, das SW Update und die Analyse der Prozessdaten. Relevante Standards in diesem Umfeld sind vor allem IEC62443, IEC61508, ISO13849, EN62061 und IEC61800-5.

Safety & Security Prozess

Figure 2 zeigt den von Assystem für das Anwendungsbeispiel angewendeten Lifecycle Prozess für sicherheitskritische Systeme.

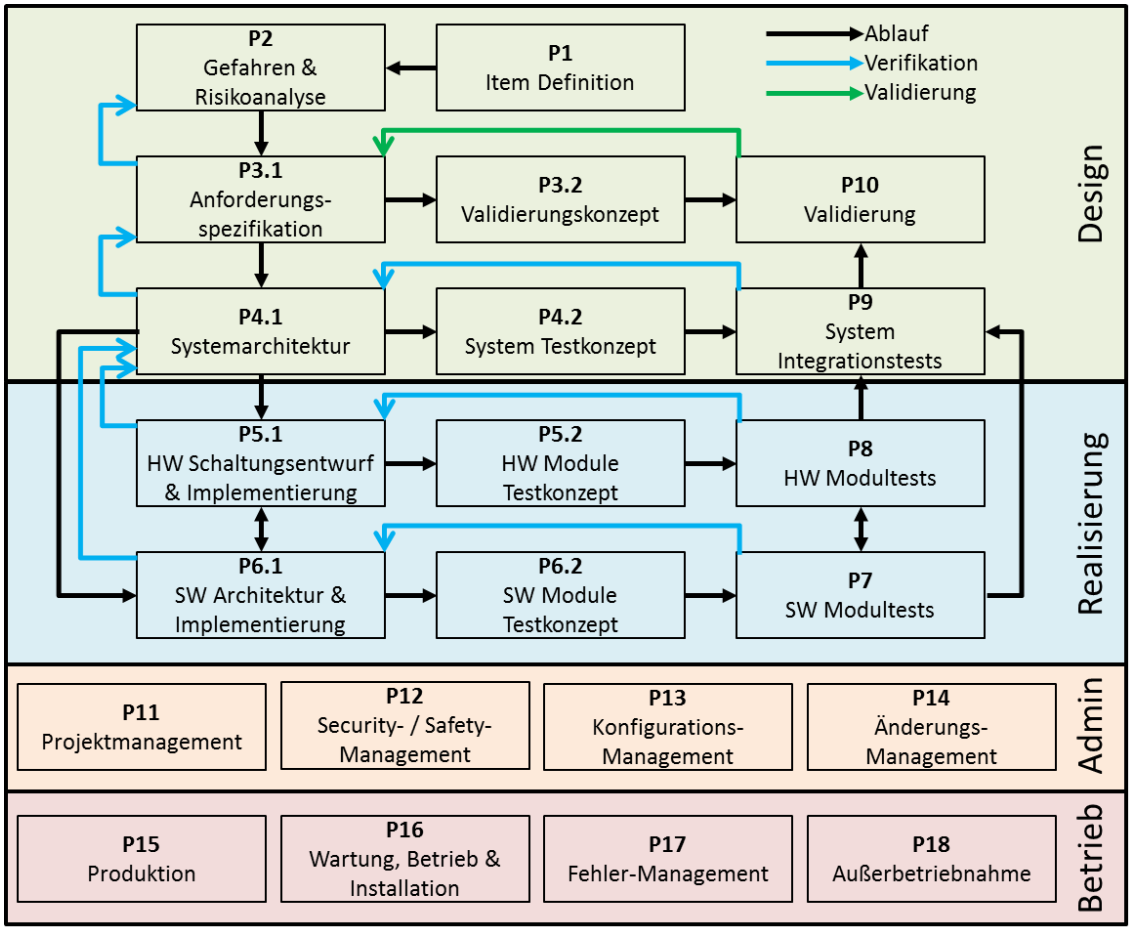

Figure 2 - Safety & Security Lifecycle Prozess

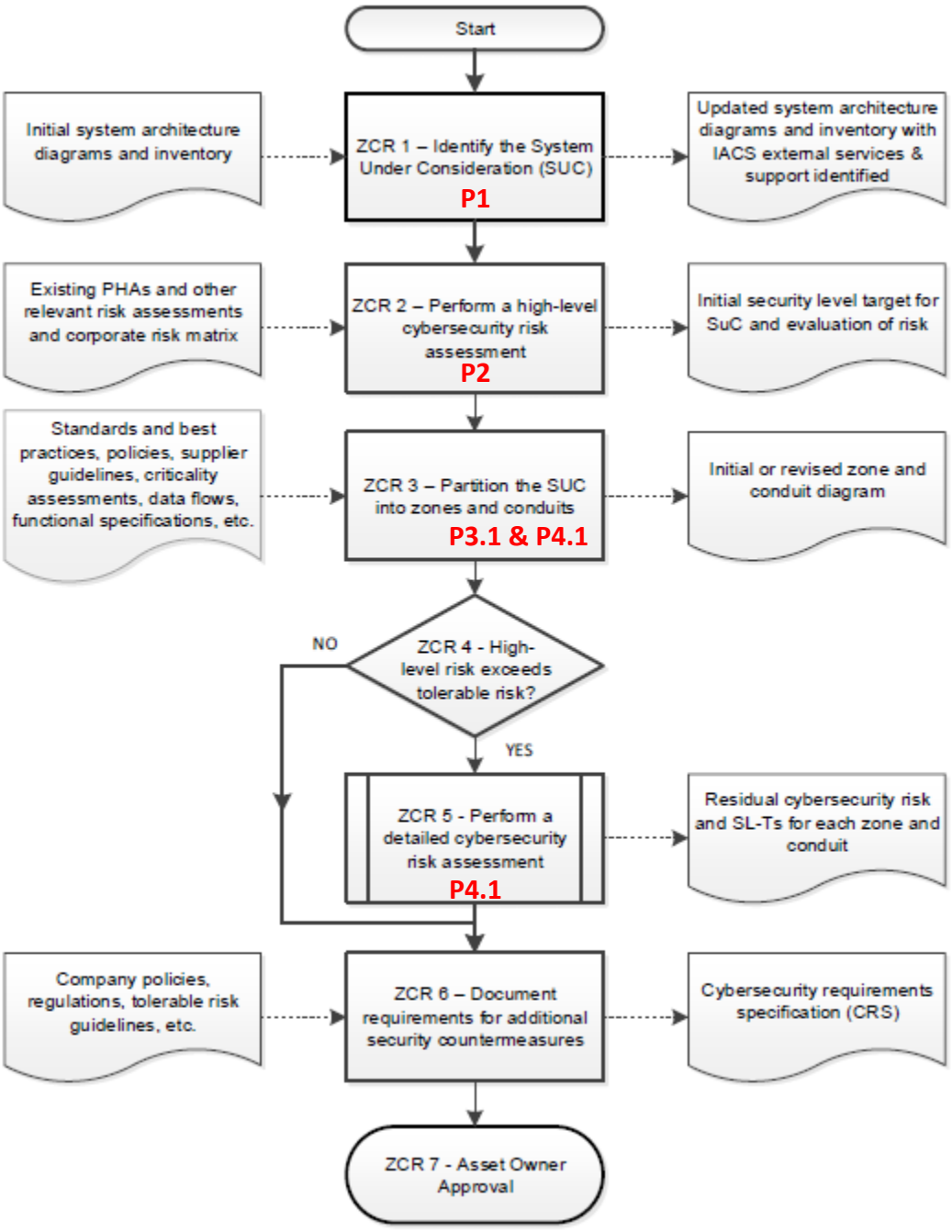

Figure 3 - Prozess Risk Assessment & Top Down Design nach IEC62443-3-2

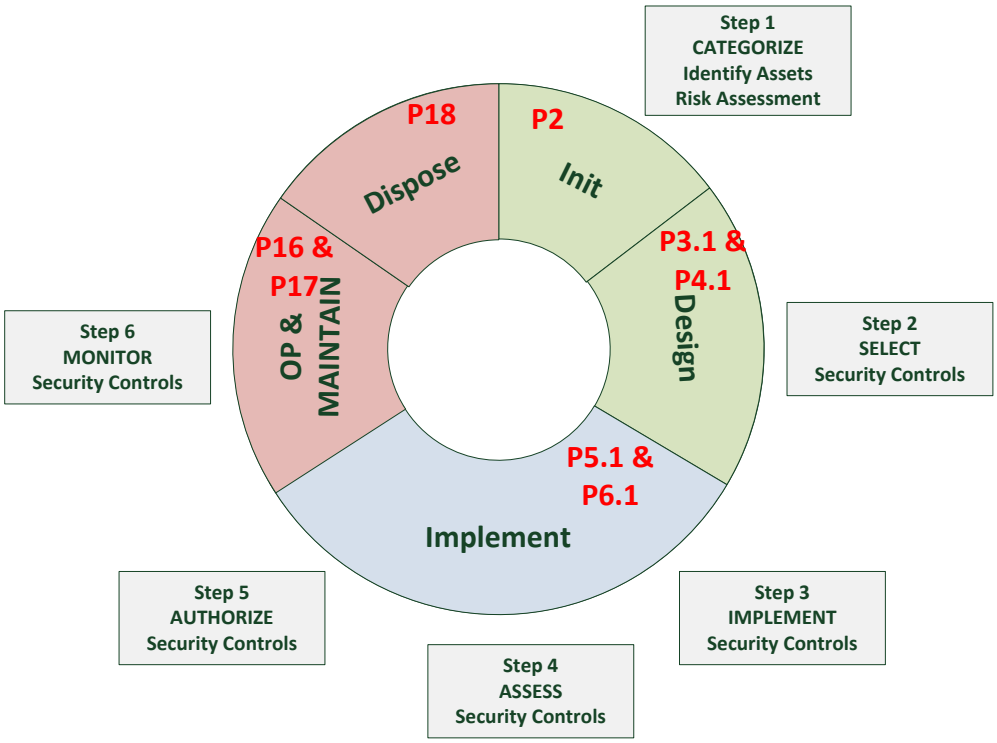

Figure 4 - Security Lifecycle nach NIST Standard

Das Mapping des Prozesses für den Top Down Entwurf nach IEC62443-3-2 ist in Figure 3 und des Prozesses „Security Lifecycle“ nach NIST Standard ist in Figure 4 dargestellt. Damit ergibt sich ein generischer Entwicklungs- und Wartungsprozess, der sowohl zu relevanten Safety Standards als auch zu den relevanten Security Standards kompatibel ist.

Die Entwicklungsphase des Lifecycle Prozesses Figure 2 ist in den Bereiche „Design“, „Realisierung“ und „Admin“ gegliedert. Der Bereich „Betrieb“ stellt die operative Phase dar. Für jeden Block sind entsprechende Input-/Output Artefakte, Verantwortlichkeiten bzw. Rollen und Aktivitäten beschrieben.

Entscheidend ist, dass die Safety bezogene Systementwicklung von der Security bezogenen Systementwicklung ab Phase P4.1 durch geeignete Systempartitionierung unabhängig erfolgen kann.

Security Risikoanalyse - Methodik & Normen am Beispiel
Nach Definition des „System under Consideration“ (SuC), wird eine High Level Risikoanalyse für wesentliche Schützgüter (Assets) des SuC durchgeführt unter Berücksichtigung der physischen Schnittstellen, Stakeholder und der Use-Cases in der geplanten Systemumgebung (vgl. Table 1).

Assets	Impact Class (CIA)	Threat Source (Motivation:	Threat (Event) (what, when)	Likelihood of Attack Initiation	Vulnerability / Attack Vector Rationale	Overall Likelihood	Impact	Impact Level	Risk	HL Security Control	Security Level Target	Mitigated Risk
Safety Funktion STO (SIL3) - SW & Konfiguration	I, A	Autorisierter Nutzer innerhalb OT Netzwerk (Mitarbeiter)	Manipulation der Safety Funktion	Possible	Physische Zugangskontrolle unzureichend z.B. durch gemeinsam genutzten Code	Unlikely	Drehmoment trotz STO aktiv, Verfügbarkeit, Fehlfunktion	Catastrophic	Moderate	IAC, UC, RDF (Physisch)	SL 3	Very Low
Safety Diagnose STO (SIL2) - SW und Konfiguration	I	Wartungs-Ingenieur innerhalb OT Netzwerk (Mitarbeiter)	Zugriff über Hardware Schnittstelle z.B. Debug Interface	Possible	Hardware Schnittstelle zugänglich ohne AC und ohne Integritäts-prüfung	Unlikely	Diagnose deaktiviert	Major	Low	IAC, UC, SI, RDF	SL 2	Very Low
SW Binary	I, A	Wartungs-Ingenieur innerhalb OT Netzwerk (Mitarbeiter)	Austausch des Trust Anchor und des SW Update Binary zur Problembehebung	Possible	Infektion mit Schadcode verursacht durch Mitarbeiter oder Vernetzung	Possible	Diagnose deaktiviert, Verfügbarkeit, Fehlfunktion	Major	Moderate	IAC, UC, SI, RDF	SL 2	Very Low
Prozessdaten "Drive Control"	C	Nicht autorisierter Zugriff von Außen	Auslesen der Prozessdaten durch Einschleusen von Malware	Possible	Schwachstelle der Zugangskontrolle oder nicht betrachtete logische Schnittstelle	Unlikely	Offenlegung des Nutzungsprofils bzw. der Prozessdaten	Minor	Low	IAC, UC, RDF	SL 1	Very Low

Table 1 - Beispiel einer High Level Risiko Analyse

Dabei werden potentielle Bedrohungen, Schwachstellen und Auswirkungen im Falle eines Exploits je Assetgruppe analysiert. Bedrohungen und Schwachstellen wird zunächst qualitativ eine Wahrscheinlichkeit zugeordnet. Der potentielle Schaden (Auswirkung) wird ebenfalls qualitativ abgeschätzt. Die qualitativen Werte der Wahrscheinlichkeit und des Schadens müssen vor Erstellung der Risikoanalyse definiert werden (vgl. Rationale in Figure 5). Beispielsweise wird eine Manipulation der Safety Funktion als katastrophal eingestuft und die Bestimmung der Wahrscheinlichkeit wird in Relation zur Anzahl der Controller im Feld und einer Zeitspanne gesetzt.

			Impact				
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
		Rationale	**-**	**Verlust Prozessdaten**	**Controller nicht verfügbar (Non-Safety)**	**Manipulierte Diagnose Safety Funktion**	**Versagen SIL3 Safety Funktion durch Manipulation**
Likelihood	**certain (>90%)**	Controller im Feld innerhalb	Low	Moderate	High	Extreme	Extreme
	Likely (50-90%)	über alle Controller im Feld innerhalb von 5 Jahren	Very Low	Low	Moderate	High	Extreme
	Possible (10-50%)	über alle Controller im Feld innerhalb von 5 Jahren	Very Low	Low	Moderate	Moderate	High
	Unlikely (3-10%)	über alle Controller im Feld innerhalb von 5 Jahren	Very Low	Low	Low	Low	Moderate
	Rare (<3%)	über alle Controller im Feld innerhalb von 5 Jahren	Very Low	Very Low	Very Low	Very Low	Low

Figure 5 - Risikoeinstufung

Daraus ergibt sich im ersten Schritt ein qualitatives Risiko je Assetgruppe. Je Assetgruppe werden dann Foundational Requirements (FRs) festgelegt zur Risikoreduktion. Den Foundational Requirements wird ein sogenannter Ziel Security Level (SL-T) zugeordnet gemäß Definition in Table 2.

SL-T (Target)	Bedeutung
0	Keine besonderen Anforderungen oder Schutzmaßnahmen notwendig
1	Schutz gegen **gelegentlichen oder zufälligen Verstoß**
2	Schutz gegen einen **absichtlichen Verstoß mit einfachen Mitteln und geringem Aufwand**, allgemeinen Fertigkeiten und geringer Motivation
3	Schutz gegen einen **absichtlichen Verstoß mit raffinierten Mitteln und mittlerem Aufwand**, automatisierungstechnischen Fertigkeiten und mittlerer Motivation
4	Schutz gegen einen **absichtlichen Verstoß mit raffinierten Mitteln und erheblichem Aufwand**, automatisierungstechnischen Fertigkeiten und hoher Motivation

Table 2 - Definition Security Level

Safety Konzept und Architektur
Die zentrale Safety Funktion des Antriebscontrollers ist die sogenannte Safe Torque Off (STO) Funktion, die eine sichere Abschaltung des Drehmoments gewährleistet. Figure 6 zeigt die zweikanalige Architektur der STO Funktion vom Eingang bis zum Ausgang. Dadurch erfüllt die STO die Anforderungen der ISO13849 für PLe und der Normen IEC61508, IEC61800-5 für SIL3. Für den Sicherheitsnachweis wird der Diagnosepfad zur Überwachung der STO Hardware Pfade separat betrachtet. Dabei wurde die Diagnose der STO Hardware Pfade einen SI Level niedriger eingestuft als die eigentliche STO Funktion und erfüllt die Anforderungen nach IEC61508 für den SIL 2.

Da der FPGA Hersteller keine quantitativen Fehleranalysen zur Verfügung stellt, wurde die Diagnosefunktion durch zwei unabhängige Pfade im FPGA realisiert. Durch zusätzliche Maßnahmen zur Erkennung bzw. Vermeidung von Common Cause Fehlern wie zu hohe oder zu niedrige Umgebungstemperatur, Versorgungsspannung, Taktung und EMV, können Einzelfehler im FPGA nicht zum Ausfall der Diagnosefunktion führen. Zusätzlich wird eine quantitativ nachweisbare hohe Safe Failure Fraction (SFF nach IEC61508) möglich.

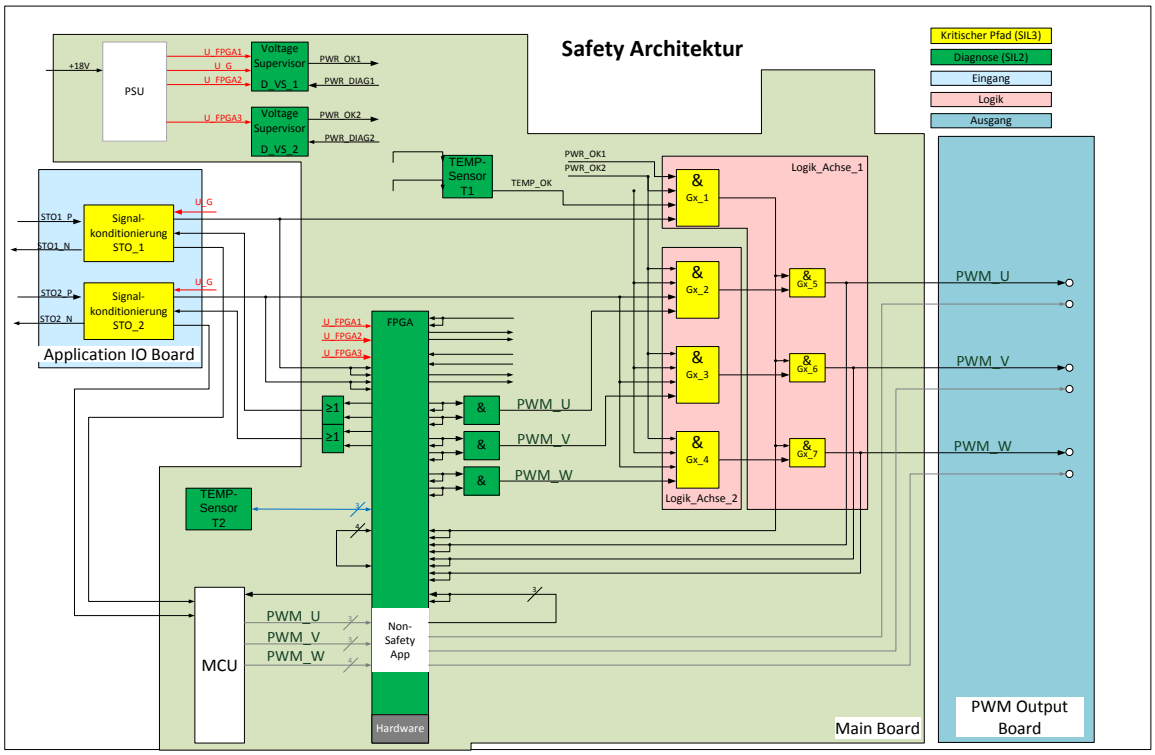

Figure 6 - Functional Safety Architektur

Security Konzept, Anforderungen und Architektur
Ergebnis der High Level Risikoanalyse auf Systemebene ist die Ableitung von Foundational Requirements (FRs) je Asset anhand der Bedrohungsszenarios. Für die einzelnen Foundational Requirements auf Systemebene wird dabei ein Ziel Security Level (SL-T) entsprechend dem erforderlichen Sicherheitsniveau festgelegt (vgl. Table 1).

FR	Bedeutung
IAC	Identification and Authentication Control
UC	Use Control (Authorization)
SI	System Integrity
DC	Data Confidentialty
RDF	Restricted Data Flow
TRE	Timely Response to Events
RA	Resource Availability

Table 3 - Foundational Requirements (FRs)

Anschließend wird eine Systemarchitektur für das zu betrachtende Systems (SuC) durch Anwendung des „Defense in Depth“ Prinzips entworfen. Dabei wird das System in sogenannte Sicherheits-Zonen und Conduits aufgeteilt. Die Aufteilung in Zonen und Conduits kann sowohl physisch als auch logisch (in Software) erfolgen und die Gruppierung erfolgt beispielsweise anhand der Kritikalität der Assets, der Funktion, des physischen / logischen Ablage-Orts oder der Zugangsberechtigung (vgl. IEC62443-3-2).

Durch den Prozess der strukturierten Risikoanalyse und Top Down Designs (vgl. Figure 3) erhält man für das Gesamtsystem (SuC) durch Anwendung des Defense in Depth Prinzips eine Aufteilung in physische und logische Sicherheitszonen (Figure 7 und Figure 8).

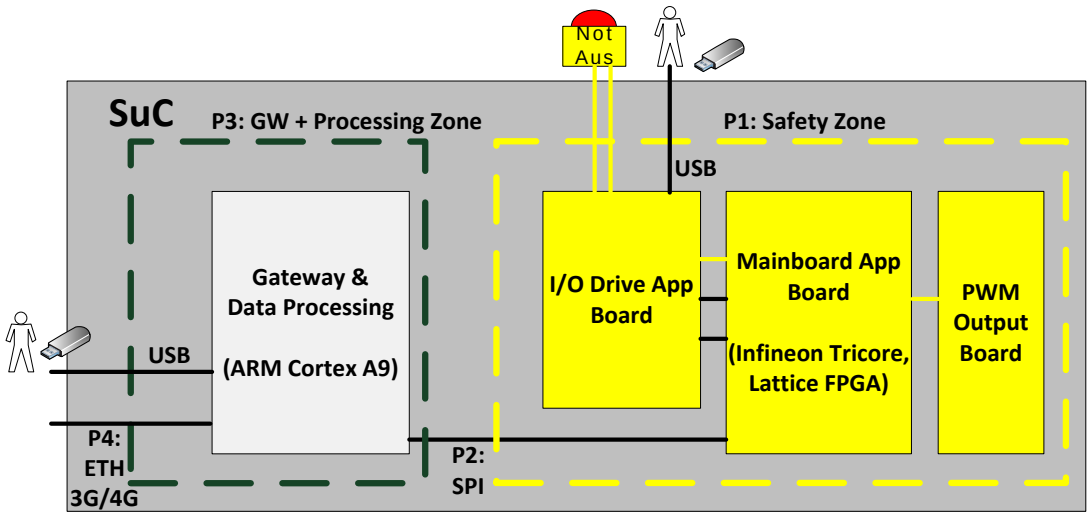

Figure 7 - Systemarchitektur mit physischen Zonen

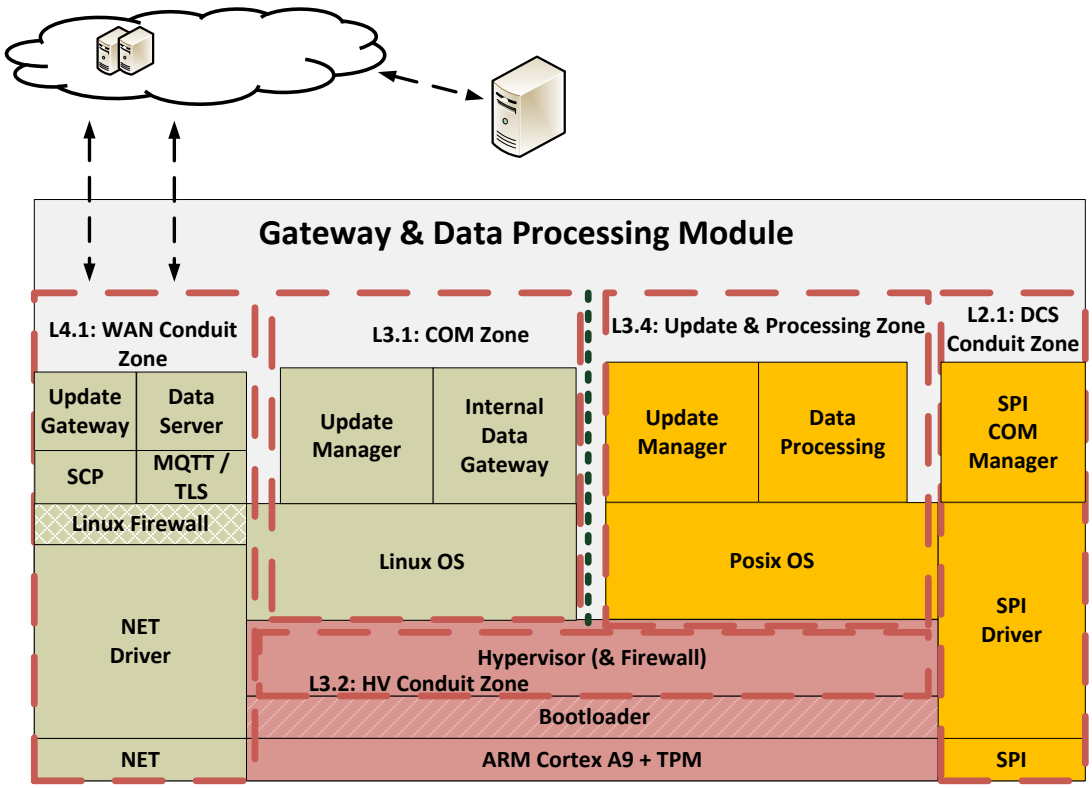

Figure 8 – Architektur des Gateway mit logischen Zonen

Jede Zone beinhaltet ein oder mehrere Systeme, die wiederum aus elementaren Komponenten bestehen. Zonen wird dabei ein bestimmter Security oder Trust Level inklusive der Foundational Requirements zugeordnet und jede Zone stellt nur die wirklich relevanten Schnittstellen nach Außen, d.h. für andere Zonen zur Verfügung. Zwischen den Zonen erfolgt in der Regel eine Authentifizierung, Verschlüsselung und Begrenzung des Datenflusses. Eingangsdaten sollten vor interner Verwendung immer validiert und Ausgangsdaten vor Ausgabe nach Möglichkeit bereinigt werden, so dass keine kritischen Informationen nach Außen preisgegeben werden.

Zusammenfassung und Ausblick

Zusammenfassend ergeben sich durch die dargestellte methodische Vorgehensweise für unser Anwendungsbeispiel zahlreiche Vorteile für Systemintegratoren und Anlagenbetreiber. Der Controller kann durch den damit erreichten hohen Sicherheitslevel und der Zertifizierung in eine Vielzahl von Anwendungen zur Ansteuerung leistungsstarker E-Motoren integriert werden. Die sichere Cloud-/Backend Anbindung ermöglicht die Vernetzung der Steuerung zur Prozessdatenanalyse sowie einfache und sichere Updates im Feld für Non-Safety Funktionen.
Zusätzlich kann der Controller durch das modulare Design für den jeweiligen Bedarf skaliert werden.

Quellen

z.B. Stuxnet, Triton Malware oder Ähnliches

Autor

Markus Maier ist Team- und Projektmanager bei der Assystem Germany GmbH. Er verfügt über langjährige Erfahrung in der Entwicklung funktional sicherheitskritischer Systeme in der Automobil- und Industrie-Branche und beschäftigt sich seit einigen Jahren intensiv mit dem Thema Cyber-Sicherheit, insbesondere mit der Härtung von Embedded Systemen und industriellen Steuerungen.