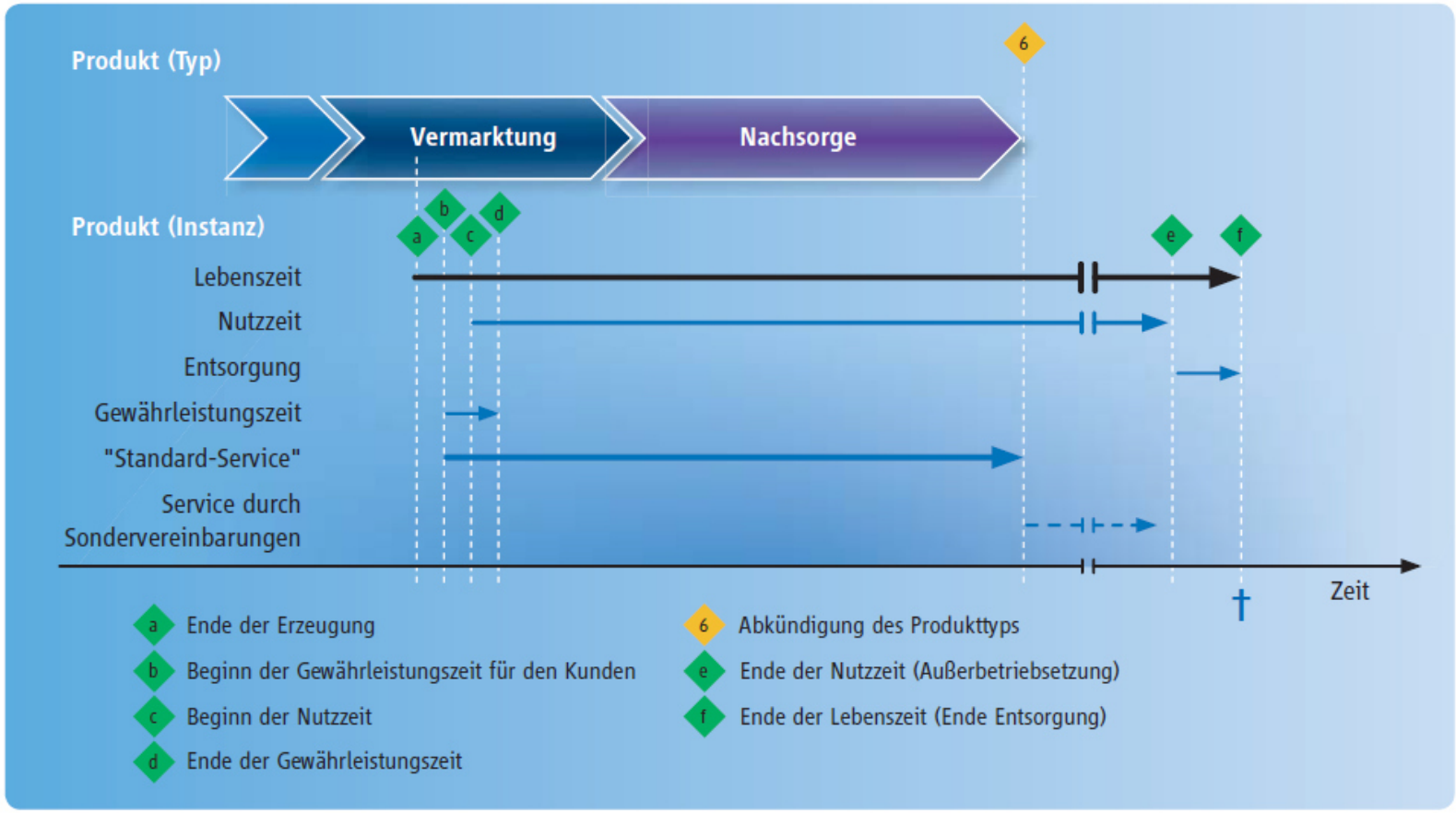
SIEMENS

„Life Cycle“ elektrischer Komponenten

Mario Fürst | Siemens Functional Safety Professional

«Life Cycle» elektrischer Komponenten



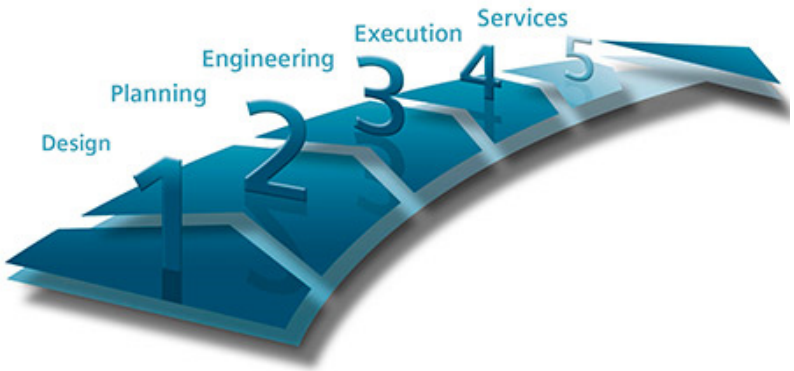
Quelle: ZVEI, Oktober 2010, Life-Cycle-Management für Produkte und Systeme der Automation – Ein Leitfaden des Arbeitskreises Systemaspekte im ZVEI Fachverband Automation

Das Lebenszyklusmodell in der IEC 61508

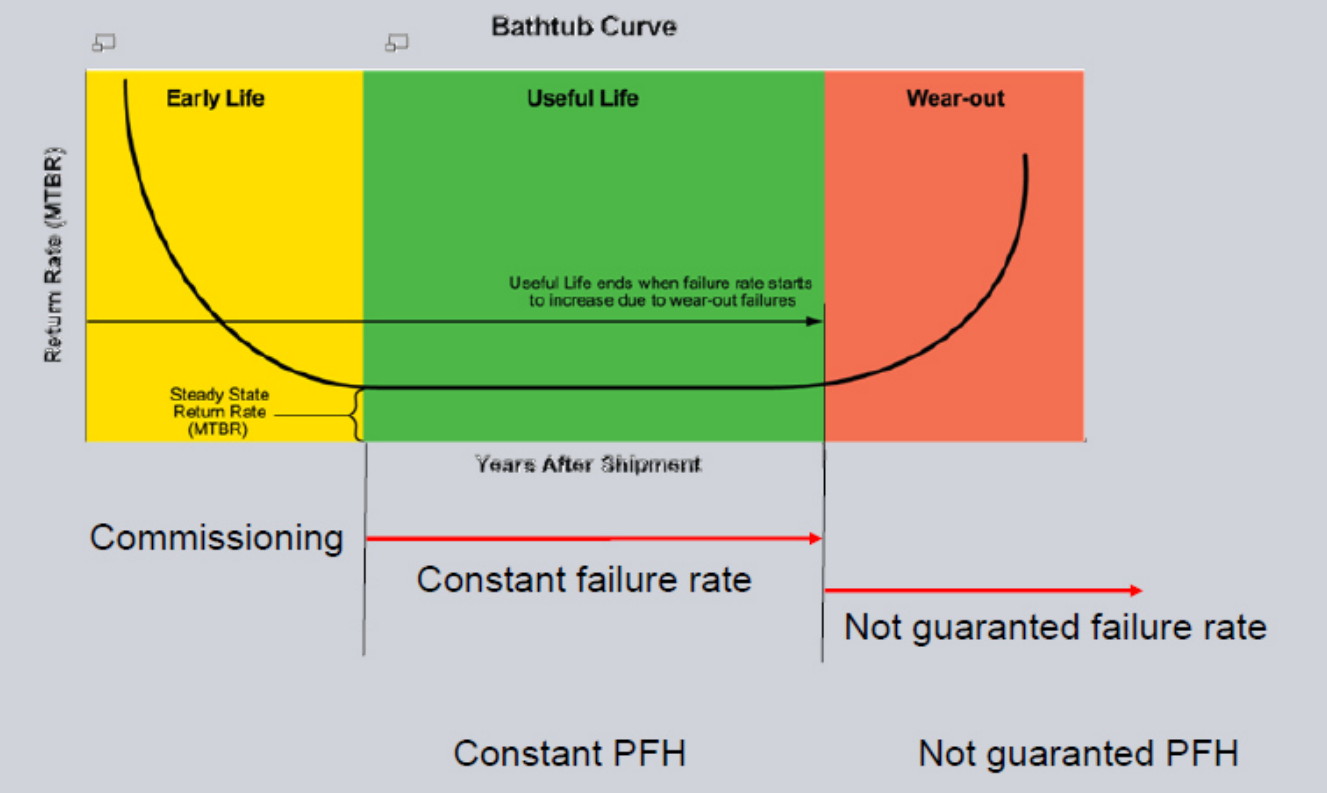
Funktionale Sicherheit

- In der IEC 61508 wird vom „**Lebenszyklus-Modell**“ ausgegangen, d. h. ein Produkt wird von der ersten Planungsstufe über die Markteinführung und das Änderungsprozedere bis hin zu seiner Ausserbetriebnahme und Entsorgung betrachtet. Über all diese **Lebensphasen** sind vom Hersteller Nachweise der Abläufe zu erzeugen, die das Produkt durchlaufen hat.

- Er hat ferner nachzuweisen, dass seine übergeordneten innerbetrieblichen Abläufe geeignet sind, Produkte herzustellen, von deren **Funktion** – auch im Versagensfall – keine unvertretbaren Schäden an Mensch, Ausrüstung und Umwelt entstehen.



«Useful life» - Badewannenkurve



SIEMENS

«Useful lifetime» gemäss IEC 61131-6, Kapitel 9.4.8

9.4.8 HW implementation

The FS-PLC shall be implemented according to the FS-PLC HW design.

During the design and development process, the following information shall be compiled by the FS-PLC manufacturer and shall be available for assessment:

a) a specification of those functions and interfaces which can be used by safety functions, e.g. application constraints, communication limitations;

b) estimates of random hardware failure rates which could cause a dangerous system failure and which are detected by diagnostic tests, see 9.4.4;

c) estimates of random hardware failure rates which could cause a dangerous system failure and which are not detected by diagnostic tests, see 9.4.4;

d) environmental limits to maintain failure rate validity;

e) the mechanical and climatic environment (e.g. vibration, shock, temperature, humidity) for which the FS-PLC is intended;

f) the manufacturer declared maximum useful lifetime of the FS-PLC which shall be 20 years or less unless the FS-PLC manufacturer can justify a longer lifetime by providing evidence, based on calculations, showing that reliability data is valid for the longer lifetime.

NOTE Some individual components within a FS-PLC have known lifetimes of less than 20 years. Typical examples include: batteries, electrolytic capacitors, LEDs, etc. As necessary, the periodic replacement of these components are handled as part of the normal maintenance procedures specified by the FS-PLC manufacturer. The maximum useful lifetime limit of 20 years is intended to cover the bulk of the FS-PLC components without known lifetimes.

Mission time, ISO 13849-1 Kapitel 4.5.4

For the designated architectures, the following typical assumptions are made:

— mission time, 20 years (see Clause 10);

— constant failure rates within the mission time;

SIEMENS

Was wird unter dem „Proof-Test“ verstanden?

Proof-Test

- In einer sicherheitsrelevanten Anwendung muss sich das sicherheitsbezogene elektrische Steuerungssystem (SRECS) in einem Zustand befinden, der die aus der Risikobetrachtung festgelegte Sicherheitsintegrität garantiert.
- **Der Proof-Test ist dabei die durchzuführende Prüfung, die dies am Ende bestätigt.**
- Während der Prüfung können Fehler oder Verschlechterungen in einem Teilsystem des SRECS erkannt werden. Falls dies der Fall ist, müssen Massnahmen für das Teilsystem ergriffen werden, um das SRECS wieder in einen Zustand zubringen, der so nah wie möglich einem „**Wie-Neu-Zustand**“ entspricht.
- In jedem Fall muss die festgelegte Sicherheitsintegrität nachweislich wiederhergestellt sein und garantiert werden.

Warum ist der „Proof-Test“ so wichtig?

Proof-Test

- Der Proof-Test deckt gefährliche Fehler auf, die nicht durch Diagnose erkannt werden.
- Die Ausfallrate eines gefährlichen Ausfalls λ_D ist proportional zum Wert des Proof-Test-Intervalls T_1 : $\lambda_D \approx T_1$
- Das bedeutet: Je kleiner das Proof-Test-Intervall, desto mehr sinkt auch die Wahrscheinlichkeit eines gefährlichen Ausfalls ($PFH_D = \lambda_D \cdot 1h$).

Das wird bei einem Proof-Test geprüft

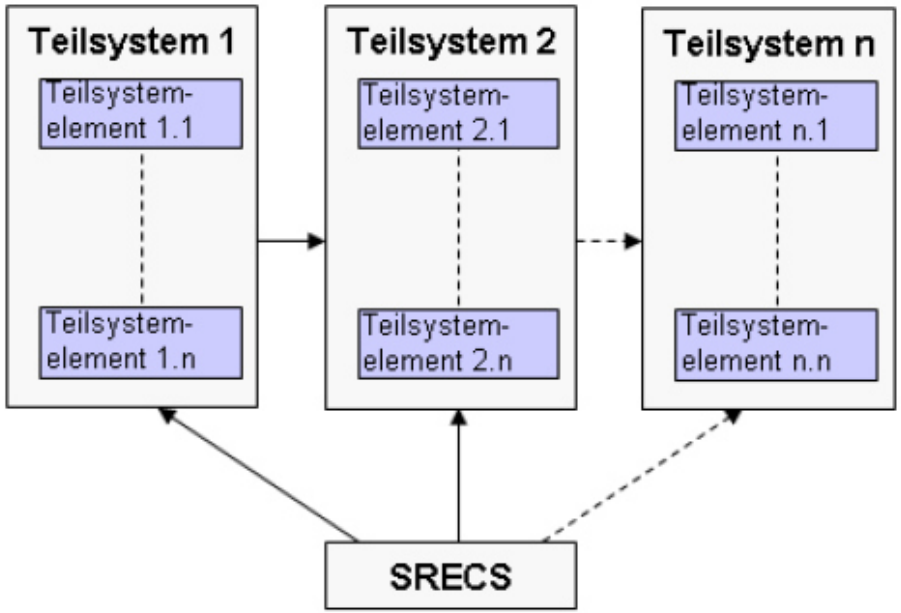
Proof-Test

Bei einem Proof-Test wird ein komplettes Teilsystem geprüft, nicht einzelne Komponenten (Teilsystem-Elemente), ausser das Teilsystem besteht nur aus einem Teilsystem-Element. Die Teilsysteme sind dabei vom Anwender selbst definiert.

Teilsystem-Elemente können sein:

Elektromechanische Komponenten (z.B. Schütze, Relais)
Wenig-komplexe elektronische Geräte (z. B. Peripherie)
Komplexe elektronische Geräte (z. B. SPS)

In jedem Fall beschränkt sich die Prüfung des Teilsystems auf die Funktionalitäten, die tatsächlich an der Sicherheitsfunktion beteiligt sind.



Was ist bei nicht-sicherheitszertifizierten Komponenten zu beachten?

Nicht-sicherheitszertifizierte Komponenten

- Bei nicht-sicherheitszertifizierten Hardwarekomponenten, die an der Sicherheitsfunktionalität beteiligt sind, müssen zudem zusätzliche Massnahmen ergriffen werden. Dabei handelt es sich z. B. um:
  - zusätzliche Diagnose (z. B. Plausibilitätsbetrachtungen)
  - redundanter Aufbau zur Erhöhung der Hardwarefehlertoleranz (HFT)
  - Diversität (empfohlen) der redundanten Hardware
    - Verwendung unterschiedlicher Hardware
    - Verwendung unterschiedlicher Messbereiche: 4 mA bis 20 mA und 0 bis 10 V

- **Im Gegensatz zu zertifizierten Sicherheitskomponenten besitzen nicht-zertifizierte Hardwarekomponenten keine charakteristischen Werte** wie
  - Ausfallrate bei gefahrbringenden Fehlern (λ_D) oder
  - Wahrscheinlichkeit gefahrbringender Hardwareausfälle pro Stunde (PFH_D)

Für die Normenberechnung nach IEC 62061 werden diese Werte allerdings auch für an der Sicherheitsfunktion beteiligte nicht-sicherheitszertifizierte Hardwarekomponenten benötigt. Auf diese Werte kann über den MTBF-Wert geschlossen werden:

Wie oft muss der Proof-Test durchgeführt werden?

Proof-Test-Intervall

- Grundsätzlich gilt: Die Hardwarekomponente (Teilsystem-Element) mit dem kleinsten angegebenen Wert für das Proof-Test-Intervall bestimmt den Zeitpunkt für die Durchführung des Proof-Tests für das Teilsystem.

- **Für die Abschätzung eines Performance Levels (PL) geht die ISO 13849-1 von einer Gebrauchsdauer von 20 Jahren aus. Für zertifizierte Sicherheitskomponenten mit einem Proof-Test-Intervall von 20 Jahren, bedeutet das, dass kein Proof-Test notwendig ist (Gebrauchsdauer = Proof-Test-Intervall).**

- Bei nicht-sicherheitszertifizierten Hardwarekomponenten gibt es keine Aussagen zum Proof-Test-Intervall. Sind diese an der Sicherheitsfunktionalität beteiligt, gilt:

    - Für das Teilsystem, in dem sich diese nicht-sicherheitszertifizierte Hardwarekomponente befindet, gilt ein Proof-Test-Intervall von einem Jahr (T1 = 1 Jahr), es sei denn es gibt Angaben zur Gebrauchsdauer oder zur MTBF, die kleiner als ein Jahr sind. Für diesen Fall würden die Angaben zu dieser Gebrauchsdauer bzw. zu dieser MTBF gelten.

    - Nach Durchführung des Proof-Test muss die nicht-zertifizierte Hardwarekomponente nicht zwangsläufig ausgetauscht werden.

Beispiel: Gebrauchsdauer = Proof-Test-Intervall

Lebens- bzw. Gebrauchsdauer

- Die Lebensdauer (bzw. Gebrauchsdauer) ist die Zeit, für die ein Gerät oder eine Baugruppe konstruktiv ausgelegt ist. Es handelt sich also um die Zeit bis zum Beginn der Verschleissphase, z.B. durch **Alterung** aufgrund chemischer Reaktionen. Bei Geräten mit elektromechanischen Teilen (Relais) wird die Lebensdauer im Wesentlichen von der Anzahl **Schaltspiele und der angeschlossenen Last** bestimmt.

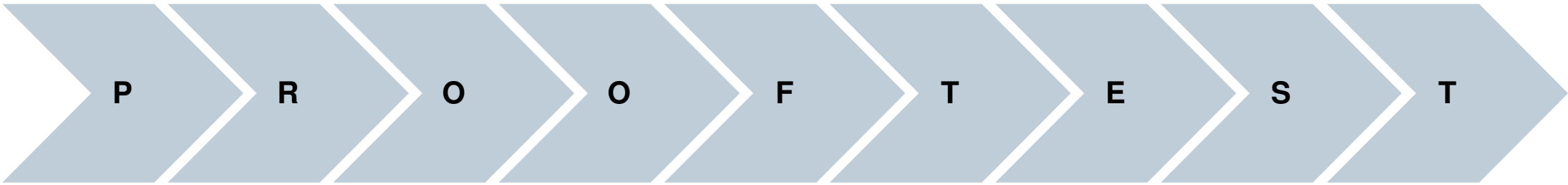
- Für elektronische Geräte ist der Punkt zur Alterung aufgrund **chemischer Reaktionen** entscheidend. Denn hier sind nicht nur die Geräte betroffen die im Einsatz sind, sondern auch die, welche auf Lager liegen. Auch für die Ersatzgeräte gilt somit die max. Gebrauchsdauer von in der Regel **20 Jahre**.

Proof-Test-Intervall und Austausch von Hardwarekomponenten

Praktische Durchführung

- Steht ein Proof-Test an, sind nicht zwangsläufig die Hardwarekomponenten (Teilsystem-Elemente) auszutauschen. Nach erfolgreichem Test dürfen diese Hardwarekomponenten (auch nicht-zertifizierte aber an der Sicherheitsfunktion beteiligte) weiter verwendet werden.
- Es ist bekannt und in jedem Fall zu berücksichtigen, dass einzelne Teilsysteme und/oder Teilsystem-Elemente (z. B. insbesondere elektromechanische Bauteile mit hohem Nutzungsfaktor) innerhalb des Intervalls für den Proof-Test des SRECS einen Austausch erfordern.
- Weiterhin sind Teilsystem-Elemente beim Proof-Test auszutauschen, wenn deren angegebene Lebensdauer (oder die angegebene MTBF) kleiner ist, als die Einsatzdauer beim nächsten Proof-Test.
  - Beispiel: MTBF = 3 Jahre; Bisherige Einsatzdauer = 2 Jahre; Proof-Test-Intervall = 2 Jahre
  - Das Teilsystem-Element muss im Proof-Test ausgetauscht werden, da:
    - MTBF < Bisherige Einsatzdauer + Proof-Test-Intervall

Praktische Durchführung des Proof-Test



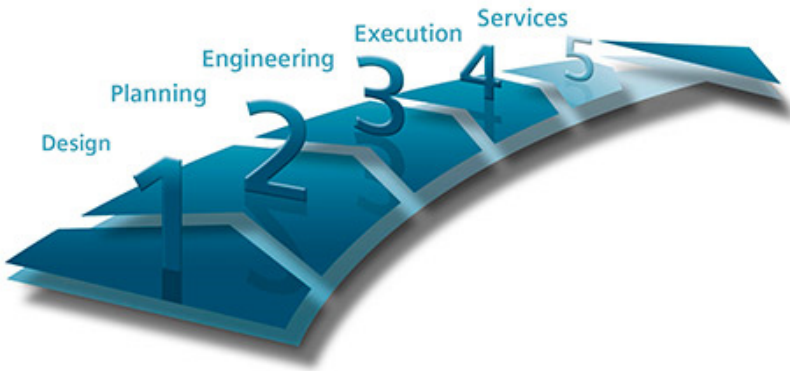
- **Zeitliche Phasen vor dem Proof-Test:**
  - Projektierungsphase (Anleitung, Klassifizierung der Testergebnisse)
  - Verifikation (Analysen und Massnahmen während der Verifikation entsprechen einem erstmalig durchgeführten Proof-Test)

- **Durchführung des Proof-Tests:**
  - Vorbereitung (Säubern, Sichtprüfung des Aufbaus, Festigkeit von Verbindungen)
  - Personen (ausreichendes sicherheitstechnisches Know-How, spezifische Berufserfahrung, Weiterbildungsmassnahmen)
  - Eingesetzte Messmittel (Messmittel in regelmässigen Abständen kalibrieren, ISO 9001)
  - Fehlerlisten (Massnahmen zur Fehlerbehebung, nachvollziehbare Argumente betreffend Fehlerausschluss)
  - Dokumentation (Dokumentation muss vollständig, widerspruchsfrei, leicht verständlich und nachvollziehbar sein)
  - Archivierung (Die Aufbewahrungspflicht besteht solange, wie die Steuerung an der Anlage betrieben wird)

Zusammenfassung

„Life cycle“ elektrischer Komponenten

- Ein proaktives Life-Cycle-Management setzt bereits im Entwurf eines Systems an. Im Fokus stehen dabei die Auswahl robuster und damit langfristig stabiler Komponenten, Spezifikationen und Technologien.
- Professionelles Life-Cycle-Management hat das Potenzial zur Differenzierung im globalen Wettbewerb.



SIEMENS

Vielen Dank für Ihre Aufmerksamkeit!

Mario Fürst | Siemens Functional Safety Professional