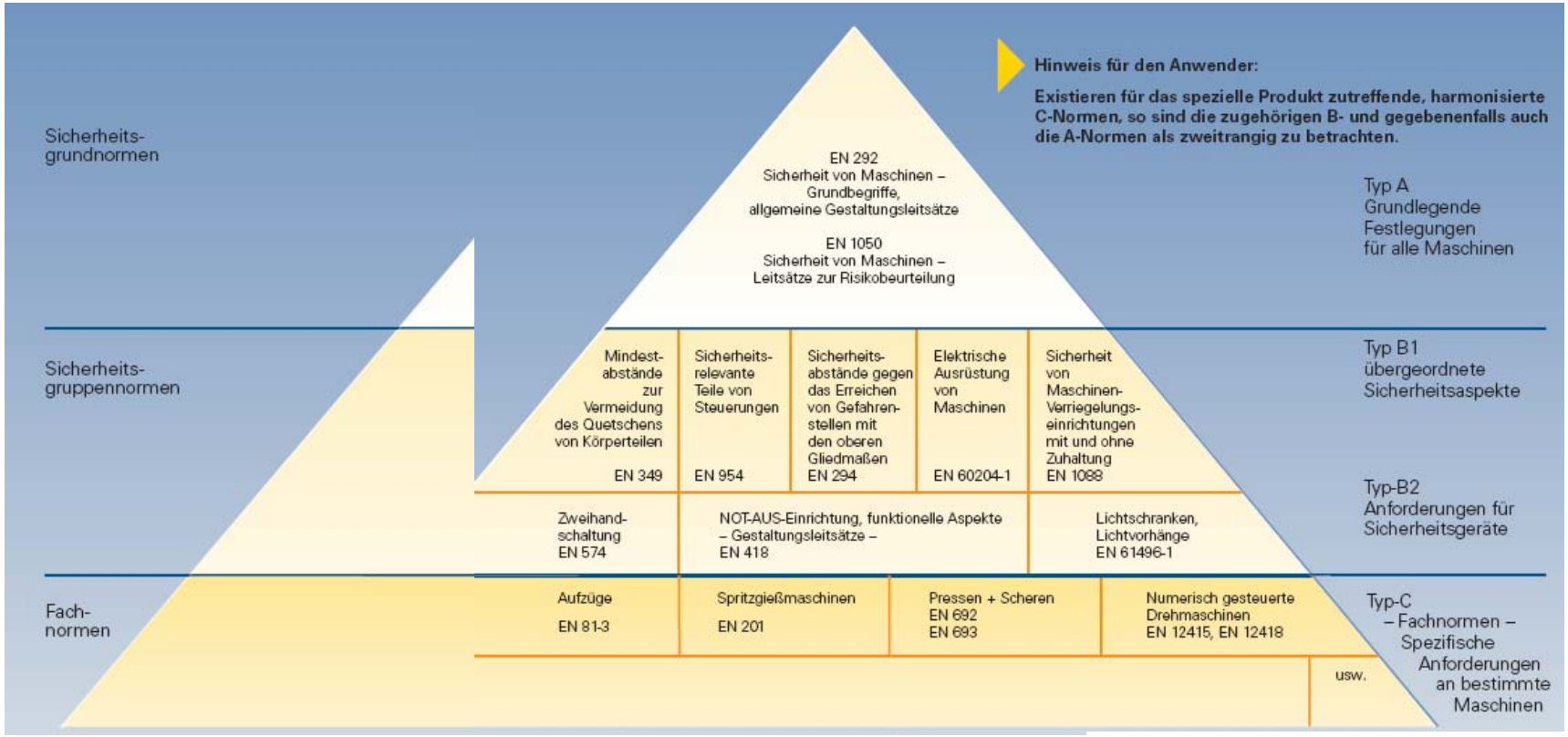
Michael Dziallas
ENGINEERING

„Das Verhüten von Unfällen darf
nicht als eine Vorschrift des
Gesetzes aufgefasst werden,
sondern als ein Gebot
menschlicher Verpflichtung
und wirtschaftlicher Vernunft.“

Werner von Siemens,
Berlin im Jahr 1880

Michael Dziallas
ENGINEERING

2.2 Normen für die Sicherheit von Maschinen



Michael Dziallas
ENGINEERING

2.3 Sicherheitsfunktionen in der Maschinensteuerung

-Ingangsetzen und Start
-Gesteuertes Stillsetzen
-Ungesteuertes Stillsetzen
-Stopp-Funktionen
-Stillsetzen im Notfall und Not-Aus-Funktionen
-Blockieren der Befehlseinrichtung
-Manuelle Rückstellung
-Start und erneuter Start
-Redundanz
-Zweihandschaltung
-Trennen von den Energiequellen
-Anforderungen an die Stellteile
-Anforderungen an die Anzeigevorrichtungen
-Muting(Aufhebung)

Michael Dziallas
ENGINEERING

2.4 Farbkennzeichnung von Drucktastern

Farbe	Bedeutung	Erklärung	Anwendungsbeispiele
ROT	Notfall	Bei gefährlichem Zustand oder im Notfall betätigen	NOT-AUS, Einleitung von NOT-AUS-Funktionen, bedingt für STOP/AUS
GELB	Anormal	Bei anormalem Zustand betätigen	Eingriff, um anormalen Zustand zu unterdrücken, Eingriff, um einen unterbrochenen automatischen Ablauf wieder zu starten
GRÜN	Sicher	Bei sicherer Bedingung betätigen oder im normalen Zustand vorzubereiten	START/EIN, hierfür jedoch bevorzugt WEISS
BLAU	Zwingend	Bei Zustand betätigen, der zwingende Handlung erfordert	Rückstellfunktion
WEISS	Keine spezielle Bedeutung zugeordnet	Für allgemeine Einleitung von Funktionen außer NOT-AUS (siehe auch Anmerkung)	START/EIN (bevorzugt), STOP/AUS
GRAU			START/EIN, STOP/AUS
SCHWARZ			START/EIN, STOP/AUS (bevorzugt)

Anmerkung: Wird eine zusätzliche Maßnahme der Kennzeichnung (z. B. Struktur, Form, Lage) zum Kennzeichnen von Drucktaster-Bedienteilen verwendet, dürfen dieselben Farben WEISS, GRAU oder SCHWARZ für verschiedene Funktionen verwendet werden, z. B. WEISS für START/EIN- und STOP/AUS-Bedienteile.

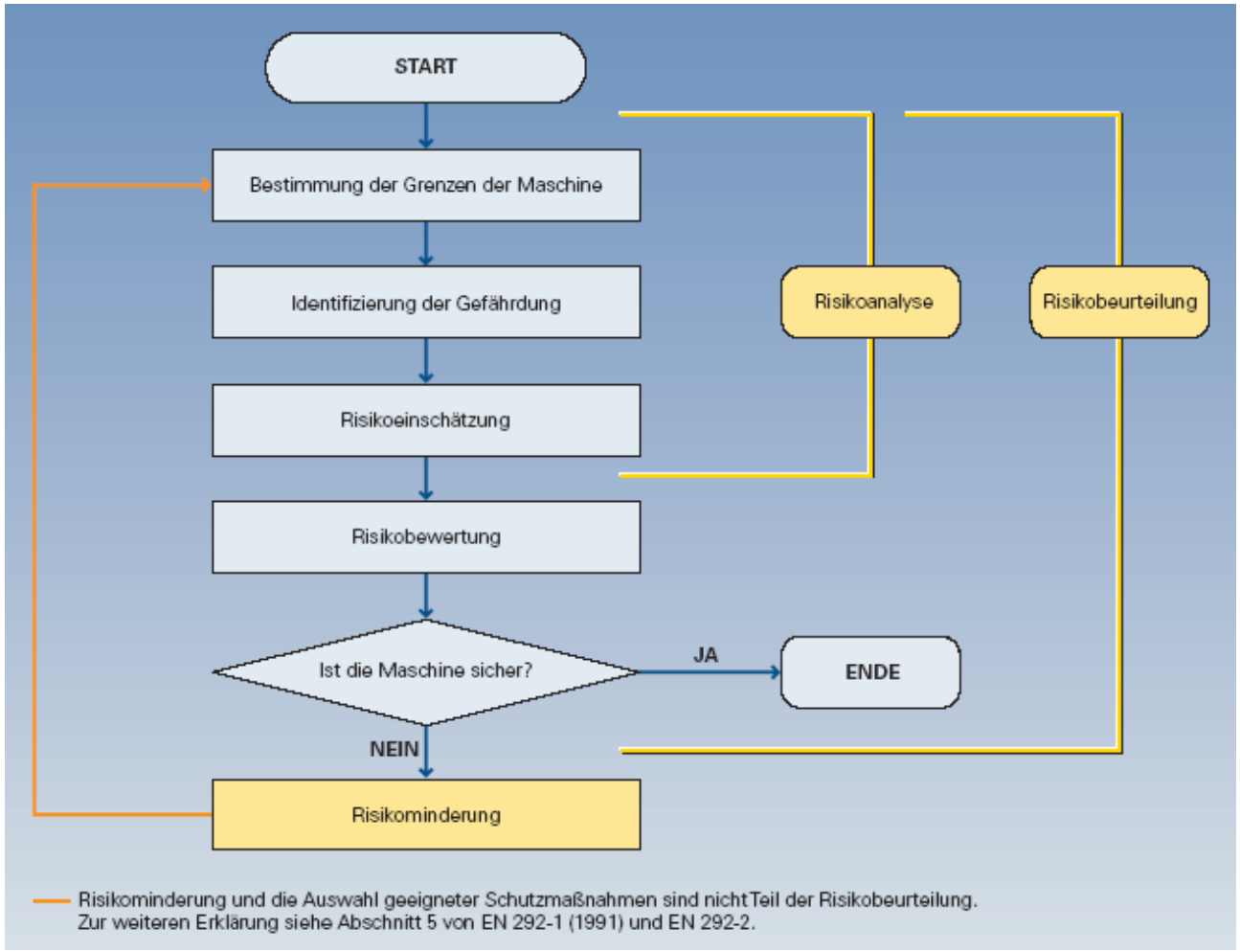
Michael Dziallas
ENGINEERING

2.4 Farbkennzeichnung von Leuchtmeldern

Farbe	Bedeutung	Erklärung	Handlung durch den Bediener	Anwendungs-beispiele
ROT	Notfall	Gefährlicher Zustand	Sofortige Handlung, um auf gefährlichen Zustand zu reagieren (z. B. durch Betätigung des NOT-AUS)	Druck/Temperatur außerhalb sicherer Grenzen, Spannungsfall, Spannungszusammenbruch, Überfahren einer Stop-Position
GELB	Anormal	Anormaler Zustand Bevorstehender kritischer Zustand	Überwachen und/ oder Eingreifen (z. B. durch Wiederherstellen der beabsichtigten Funktion)	Druck/Temperatur übersteigt normale Bereiche, Auslösen einer Schutzeinrichtung
GRÜN	Normal	Normaler Zustand	Optional	Druck/Temperatur innerhalb normaler Bereiche, Ermächtigung fortzufahren
BLAU	Zwingend	Anzeige eines Zustandes, der Handlung durch den Bediener erfordert	Zwingende Handlung	Anweisung, vorgegebene Werte einzugeben
WEISS	Neutral	Andere Zustände: darf verwendet werden, wenn Zweifel über die Anwendung von ROT, GELB, GRÜN oder BLAU bestehen	Überwachen	Allgemeine Informationen

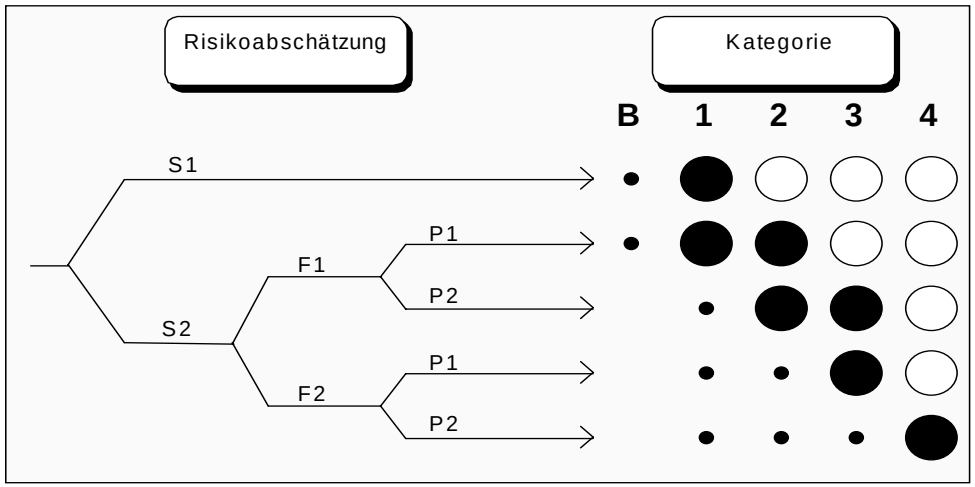
Michael Dziallas
ENGINEERING

3.1 Risikoanalyse/Risikobeurteilung



Michael Dziallas
ENGINEERING

3.1 Risikokategorien



S Schwere der Verletzung:

1 : leichte Verletzung
2 : schwere Verletzung einschließlich Tod einer Person

F Aufenthalt im Gefahrenbereich:

1 : selten bis öfters und/oder kurze Dauer
2 : häufig bis dauernd und/oder lange Dauer

P Gefahrenabwendung:

1 : möglich unter bestimmten Bedingungen
2 : kaum möglich

B Kategorien für sicherheitsbezogene Steuerungsteile:

● : bevorzugte Kategorien für die Höhe des Risikos
• : mögliche Kategorien, die zusätzlich Maßnahmen erfordern
○ : überdimensionierte Maßnahmen in Bezug auf das zutreffende Risiko

Michael Dziallas
ENGINEERING

- Maß der Safety Performance

... geforderte sicherheitsbezogene Leistungsfähigkeit (Safety Performance) ist risikoabhängig

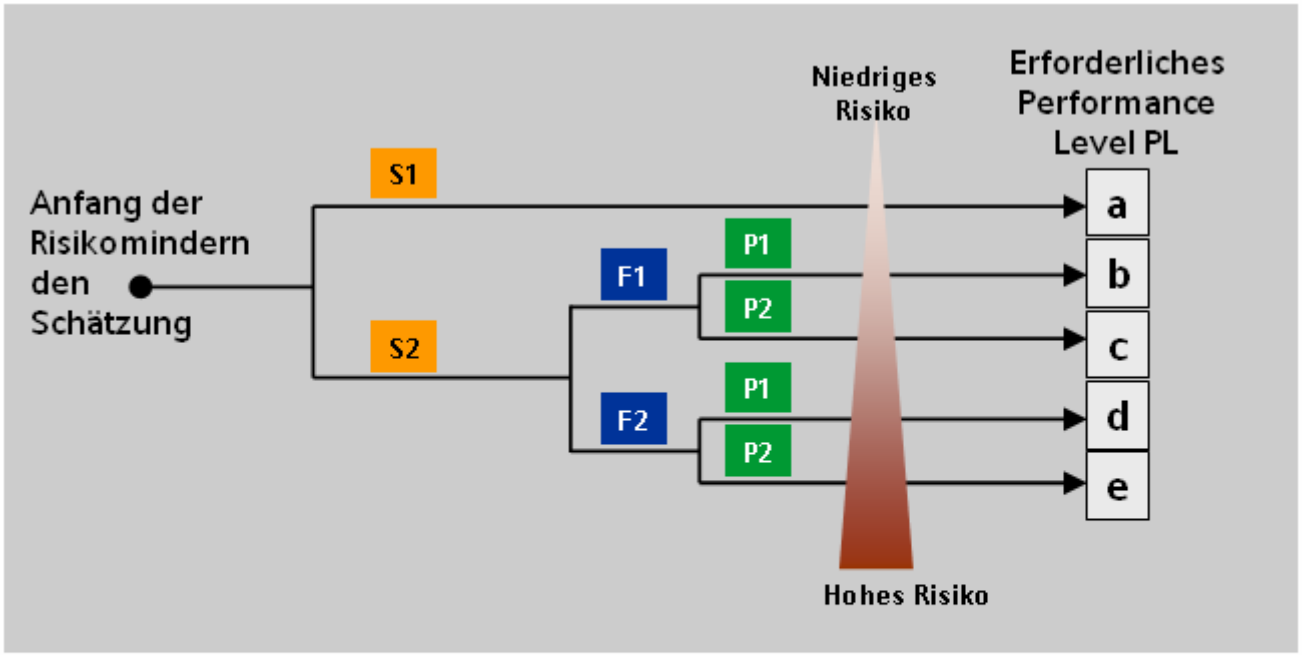
- **bisher:** Kategorie
  - Lösungsabhängig
  - Kein eindeutiger Bezug zur Höhe des Risikos
- **zukünftig:** SIL (Safety Integrity level) / PL (Performance Level)
  - Lösungsunabhängig
  - Eindeutige Abstufung nach Höhe des Risikos

Performance level (PL)	Average probability of a dangerous failure per hour [1/h]	SIL [EN 61508-1 (IEC 61508-1)] for information
a	$\geq 10^{-5}$ to $< 10^{-4}$	-
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	SIL 1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	SIL 1
d	$\geq 10^{-7}$ to $< 10^{-6}$	SIL 2
e	$\geq 10^{-8}$ to $< 10^{-7}$	SIL 3

SIL und PL_r sind aufeinander abbildbar

Michael Dziallas
ENGINEERING

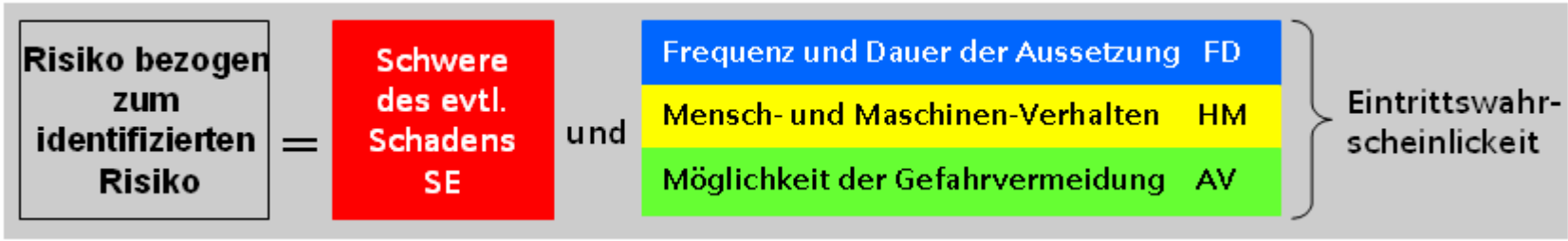
- Risikobeurteilung / Risikograph EN ISO 13849-1: 2006



Risikoparametern
S = Schwere der Verletzung
F = Häufigkeit und/oder Aufenthaltszeit in der Gefahrenstelle
P= Möglichkeit zur Vermeidung bzw. Begrenzung der Gefahr
a,b,c,d,e = Schätzung der sicherheitsbezogenen Performance Level

Michael Dziallas
ENGINEERING

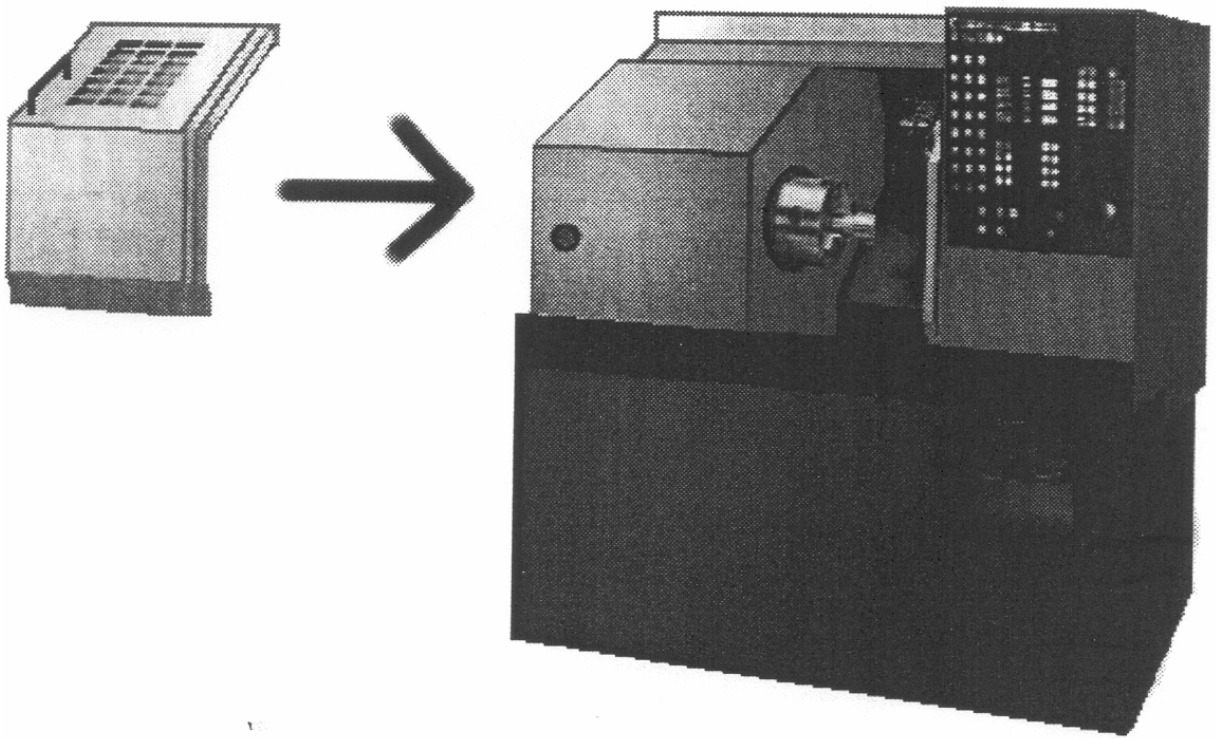
- Risikobeurteilung
  SIL assignment in draft IEC 62061, annex A



Auswirkungen	Schadens-ausmaß Se	Klasse Cl					Häufigkeit und/oder Aufenthaltsdauer Fr		Eintrittswahrscheinlichkeit des Gefährdungsereignis Pr				Möglichkeit zur Vermeidung Av	
		3-4	5-7	8-10	11-13	14-15								
Tod, Verlust von Auge oder Arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	sehr hoch	5				
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h to ≤ 1 day	5	hoch	4				
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 day to ≤ 2 weeks	4	möglich	3			unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 weeks to ≤ 1 year	3	selten	2			selten	3
							> 1 year	2	unwahrscheinlich	1			möglich	1

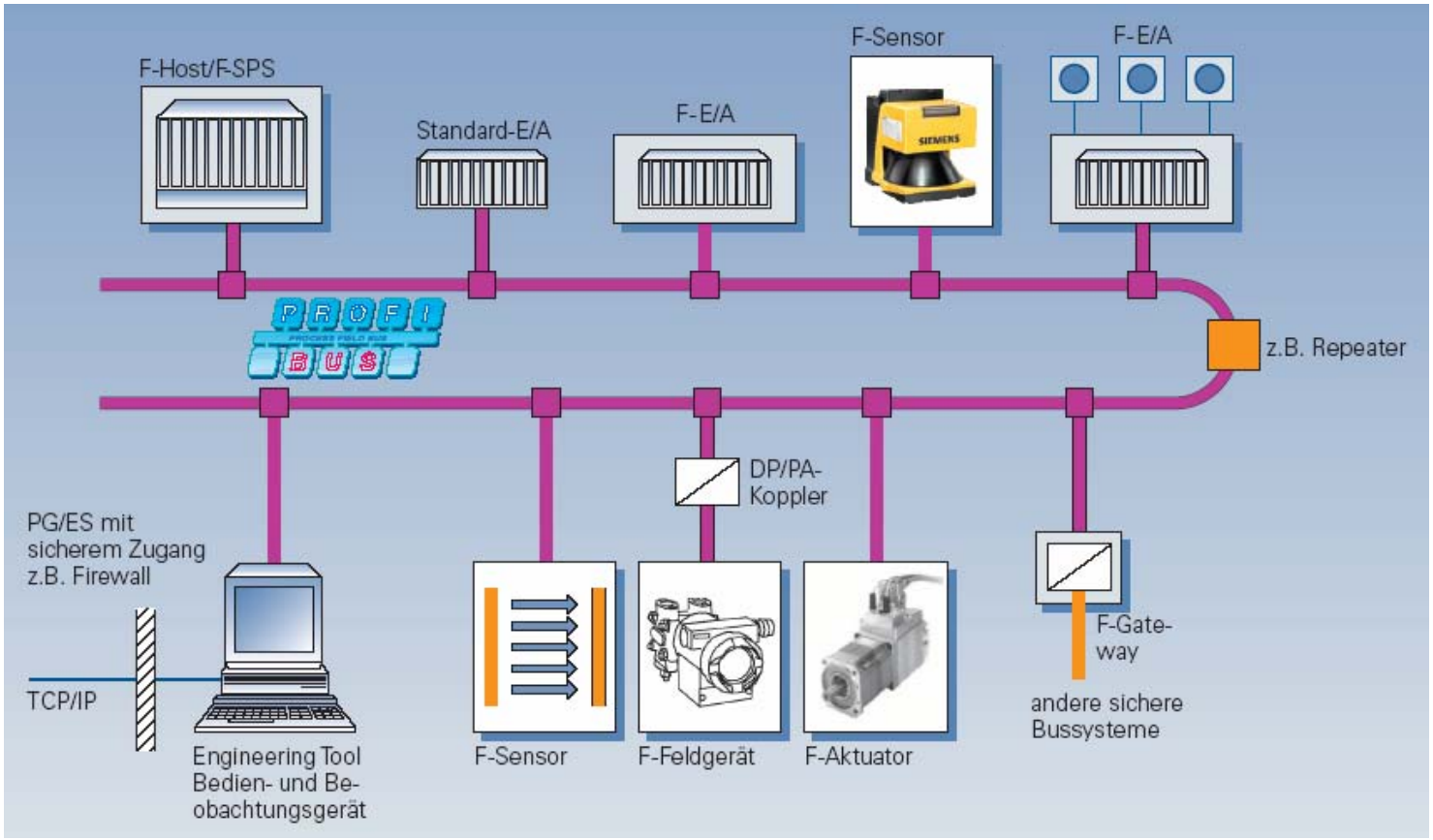
Michael Dziallas
ENGINEERING

3.2 Risikobeurteilung anhand einer CNC-Maschine



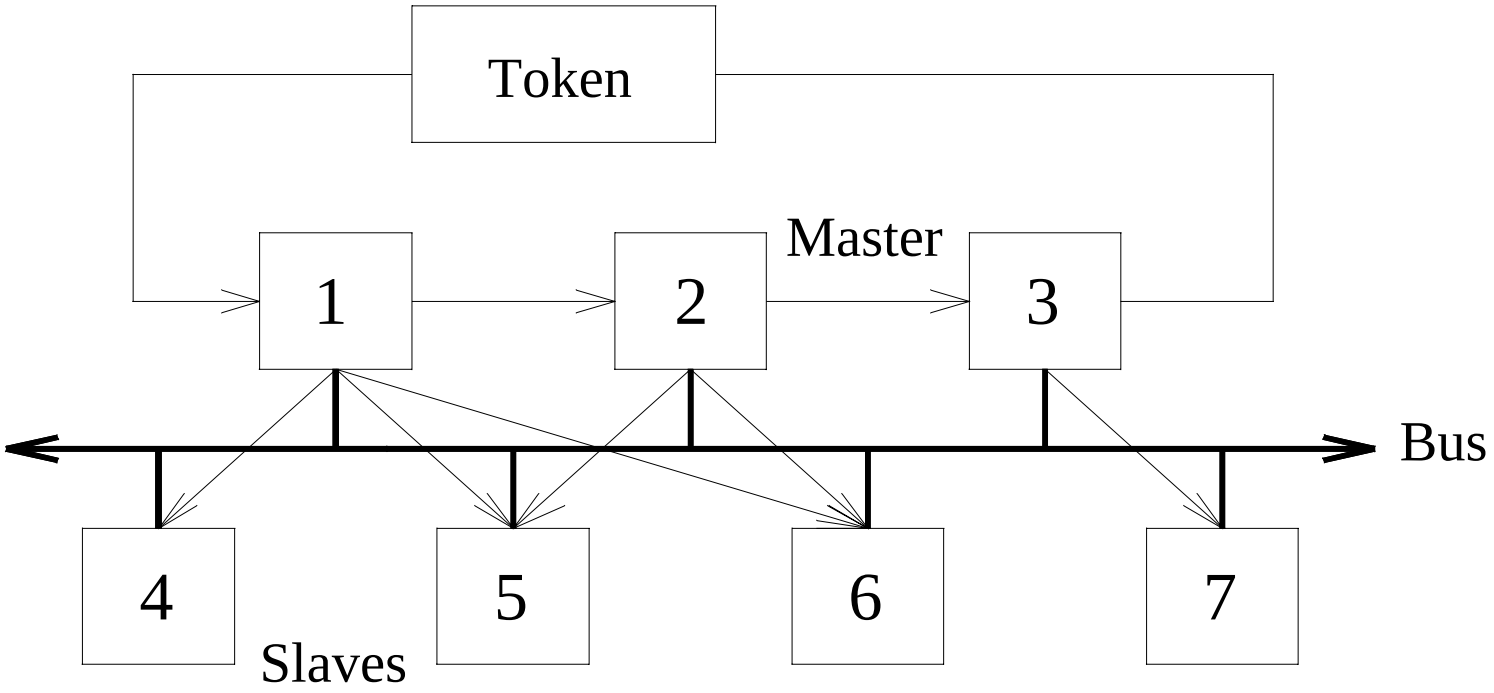
Michael Dziallas
ENGINEERING

4.2 Koexistenz PROFIsafe und PROFIBUS auf einem Kabel



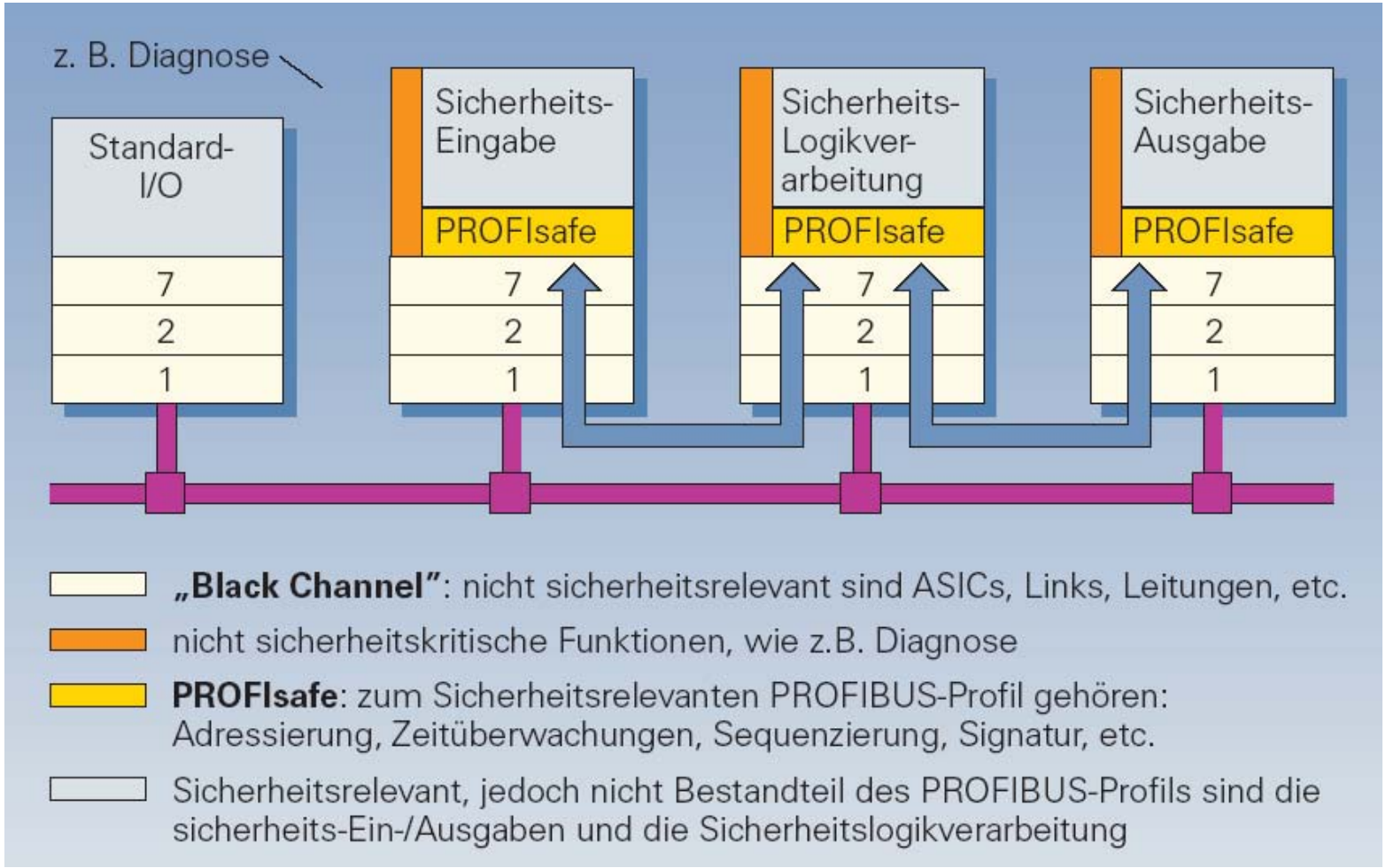
Michael Dziallas
ENGINEERING

4.2 Hybrides Zugriffsverfahren beim PROFIBUS DP



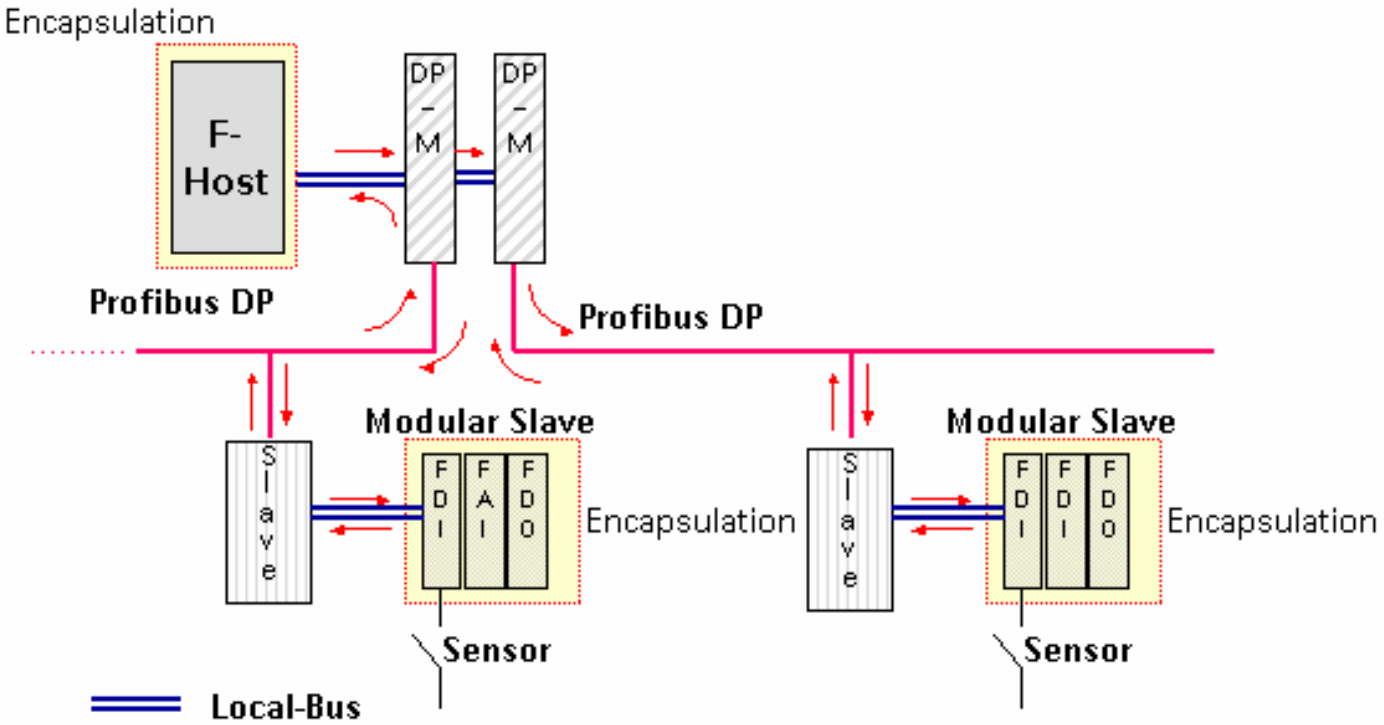
Michael Dziallas
ENGINEERING

4.2 PROFIsafe Safety-Layer



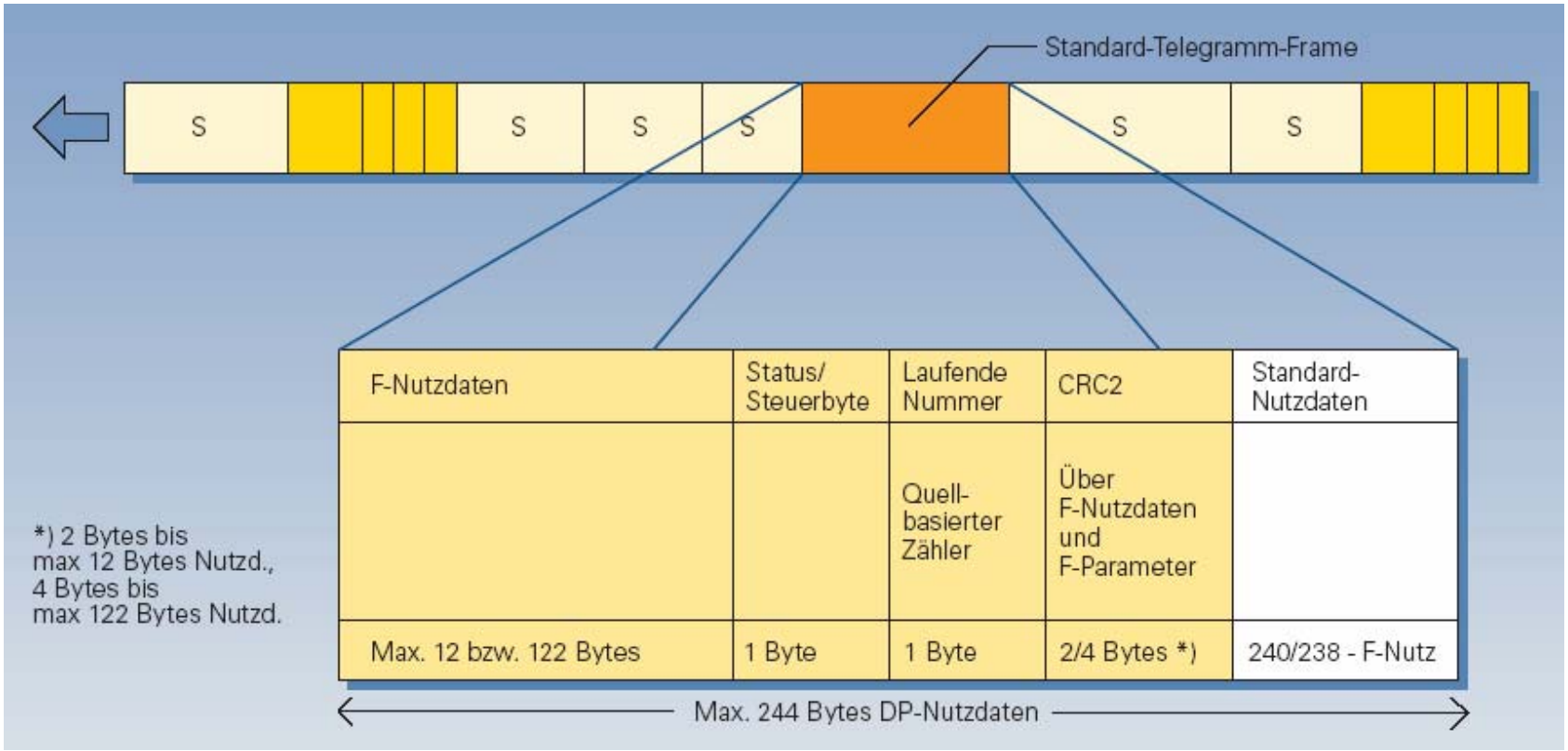
Michael Dziallas
ENGINEERING

4.2 Encapsulation



Michael Dziallas
ENGINEERING

4.2 PROFIsafe Telegramm



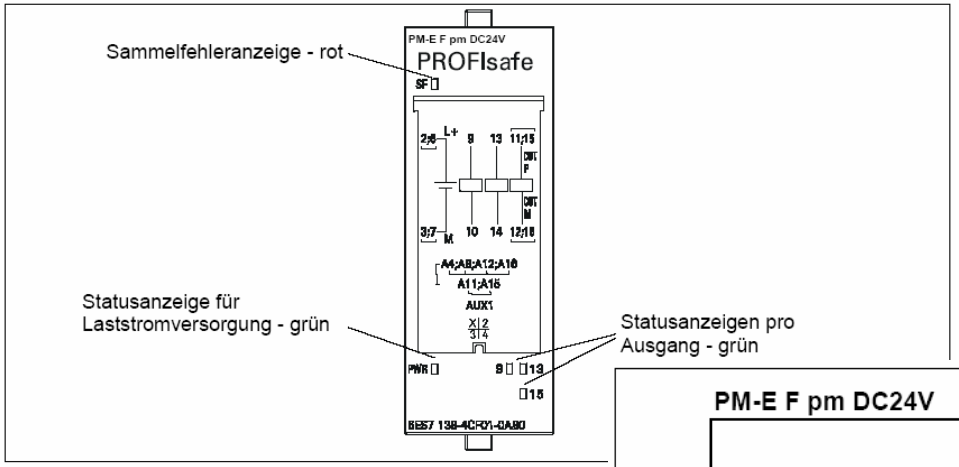
Michael Dziallas
ENGINEERING

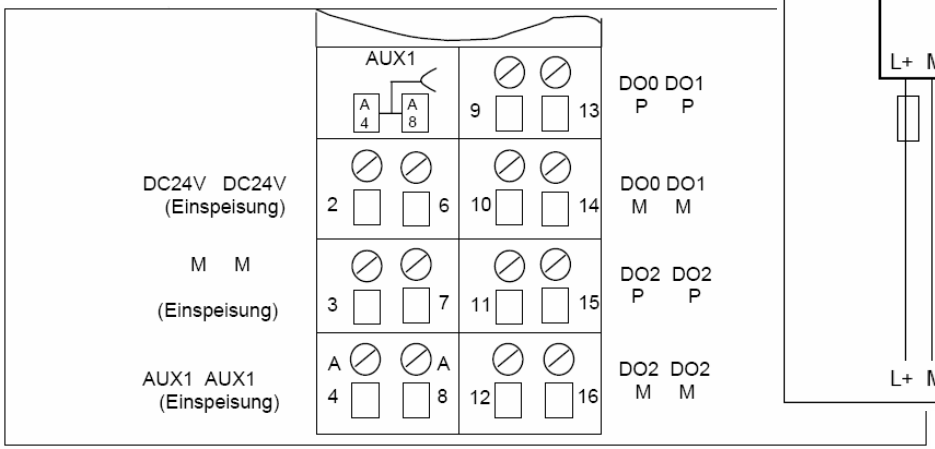
4.2 Aufdeckung der Kommunikationsfehler

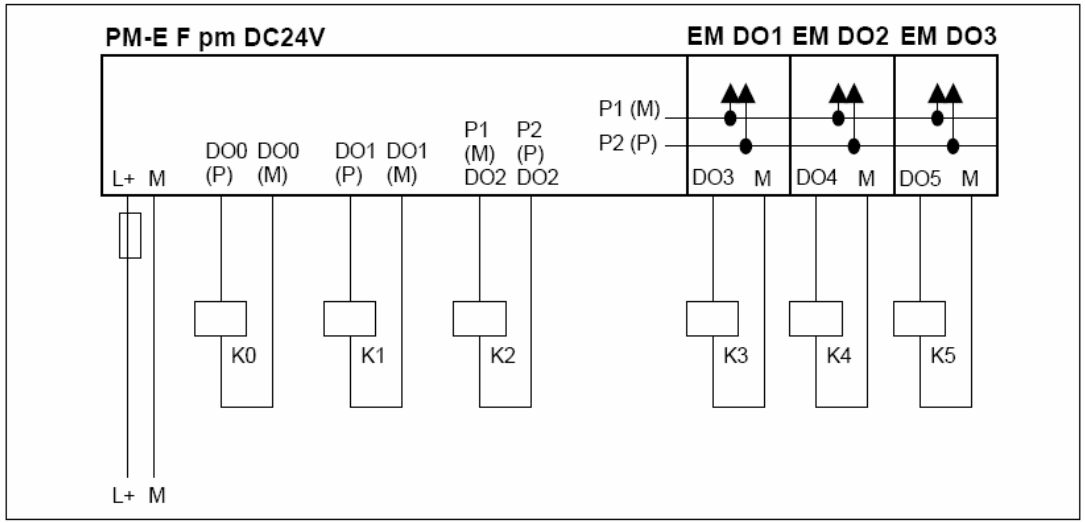
Maßnahme: / Fehler:	Laufende Nummer (Lebenszeichen)	Zeiterwartung mit Quit-tierung	Kennung für Sender und Empfänger	Daten-sicherung
Wiederholung	x			
Verlust	x	x		
Einfügung	x	x	x	
Falsche Abfolge	x			
Verfälschung von Nutzdaten				x
Verzögerung		x		
Kopplung von sicher-heitsrelevanten und Standard-Nachrichten (Maskerade), einschließ-lich Falsch- und Doppel-adressierung		x	x	x
FIFO Fehler innerhalb des Routers		x		

Michael Dziallas
ENGINEERING

4.4 F-Modul PM-E F pm DC24V

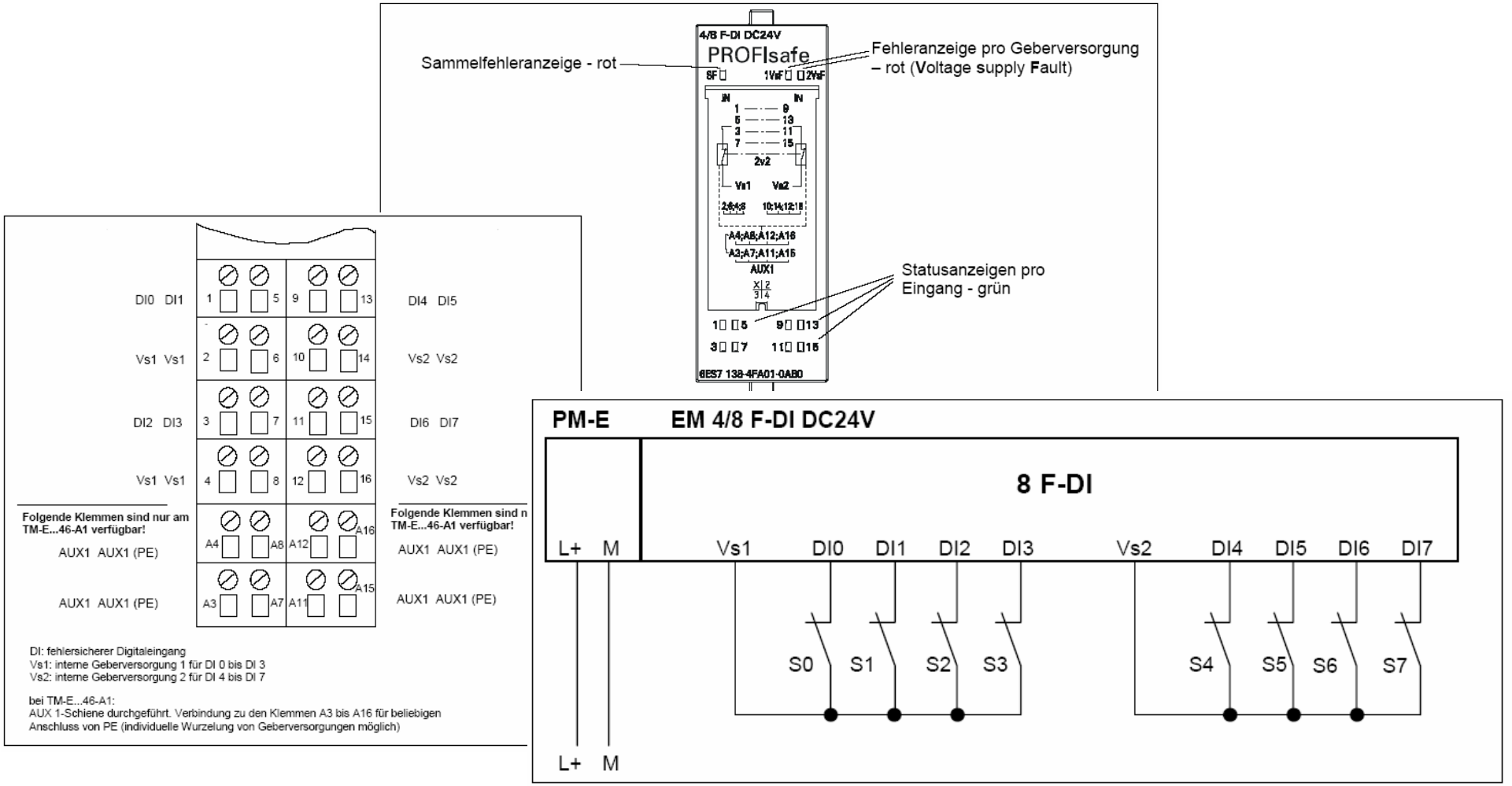






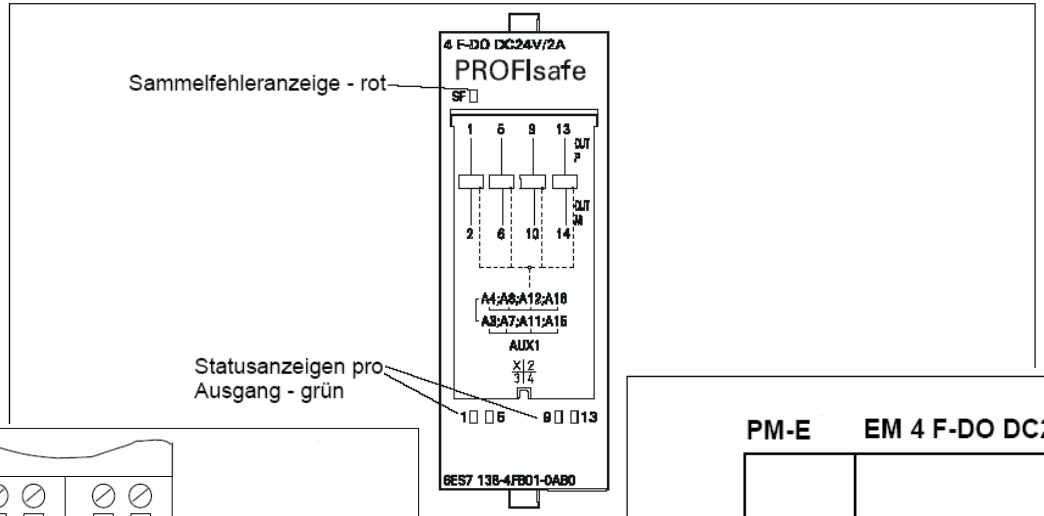
Michael Dziallas
ENGINEERING

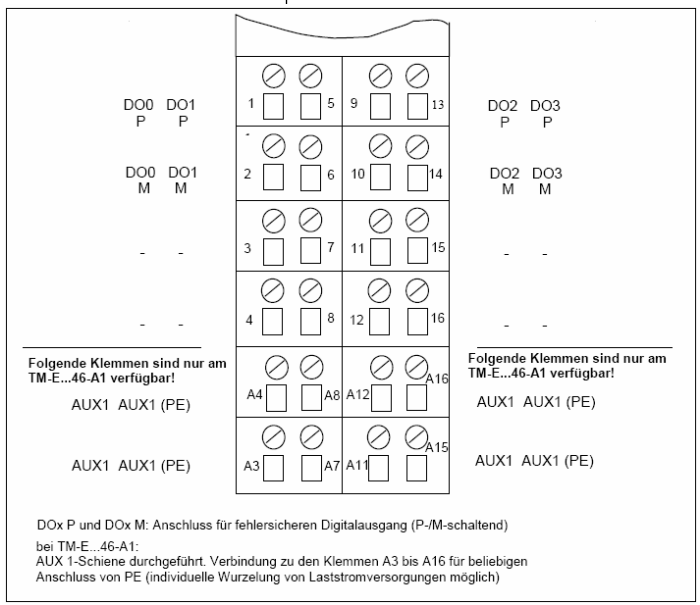
4.4 F-Modul EM 4/8 F-DI DC24V

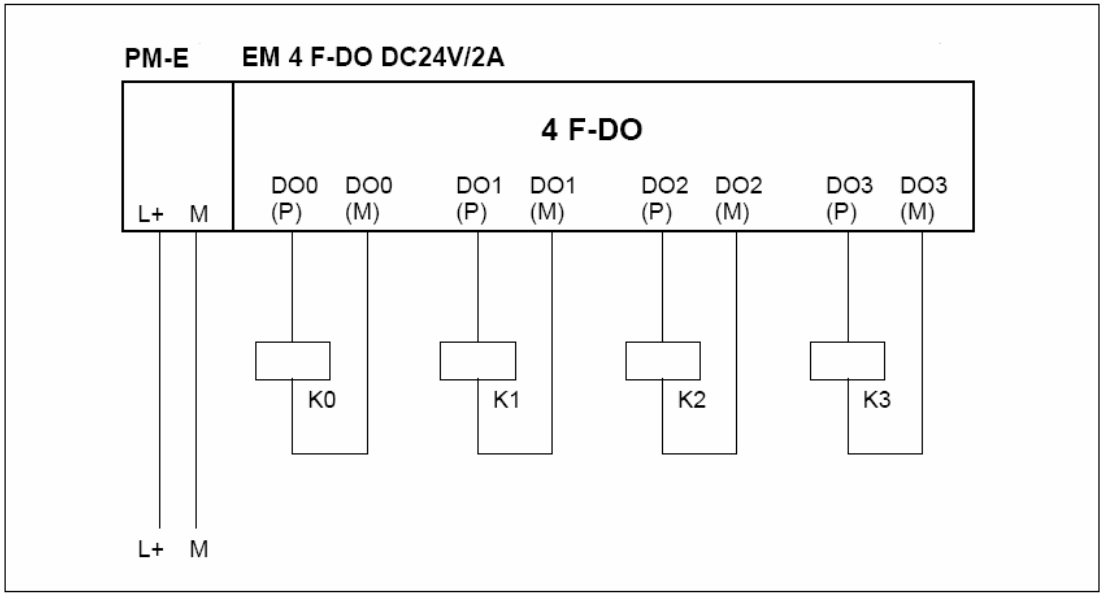


Michael Dziallas
ENGINEERING

4.4 F-Modul EM 4 F-DO DC24V/2A

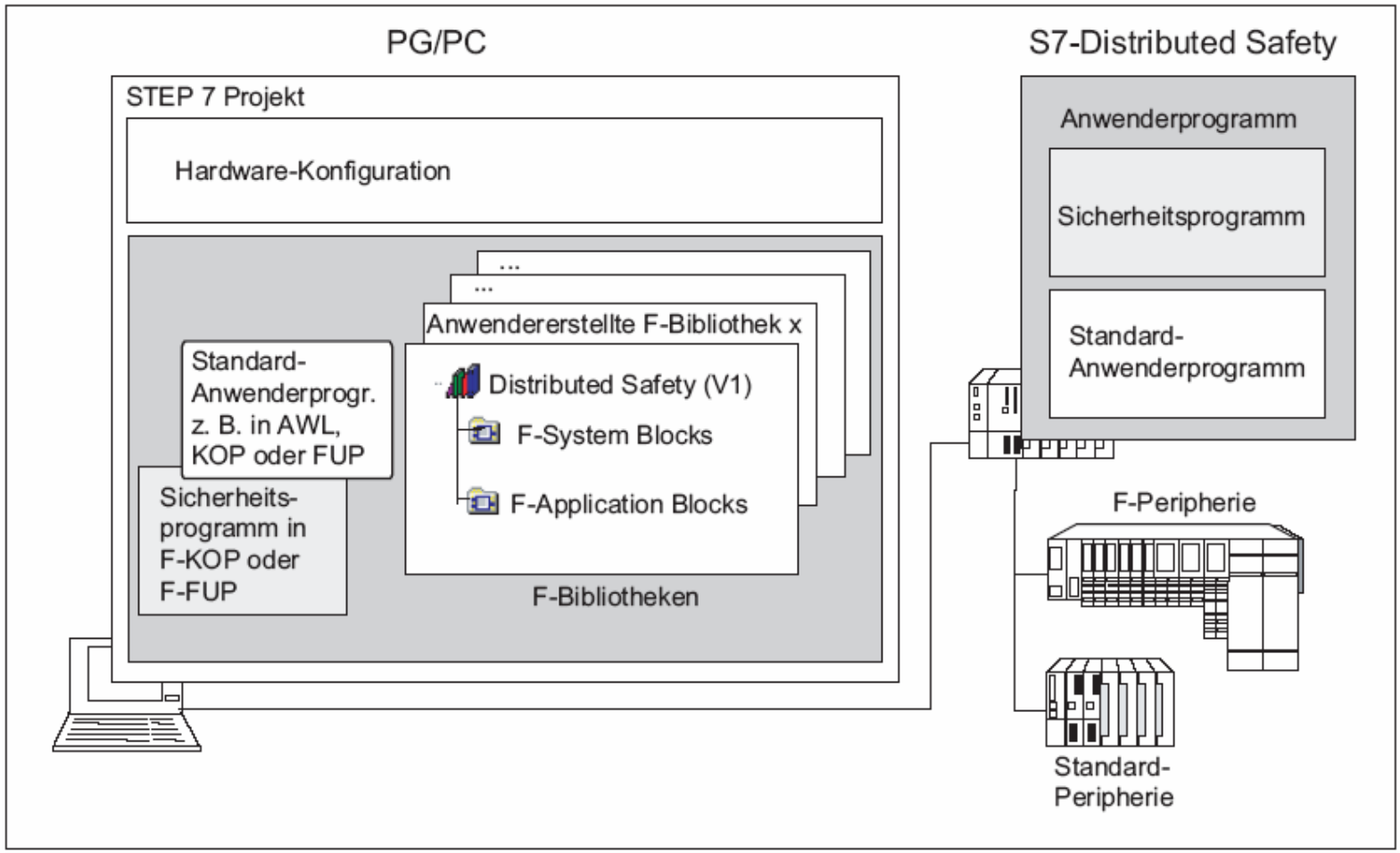






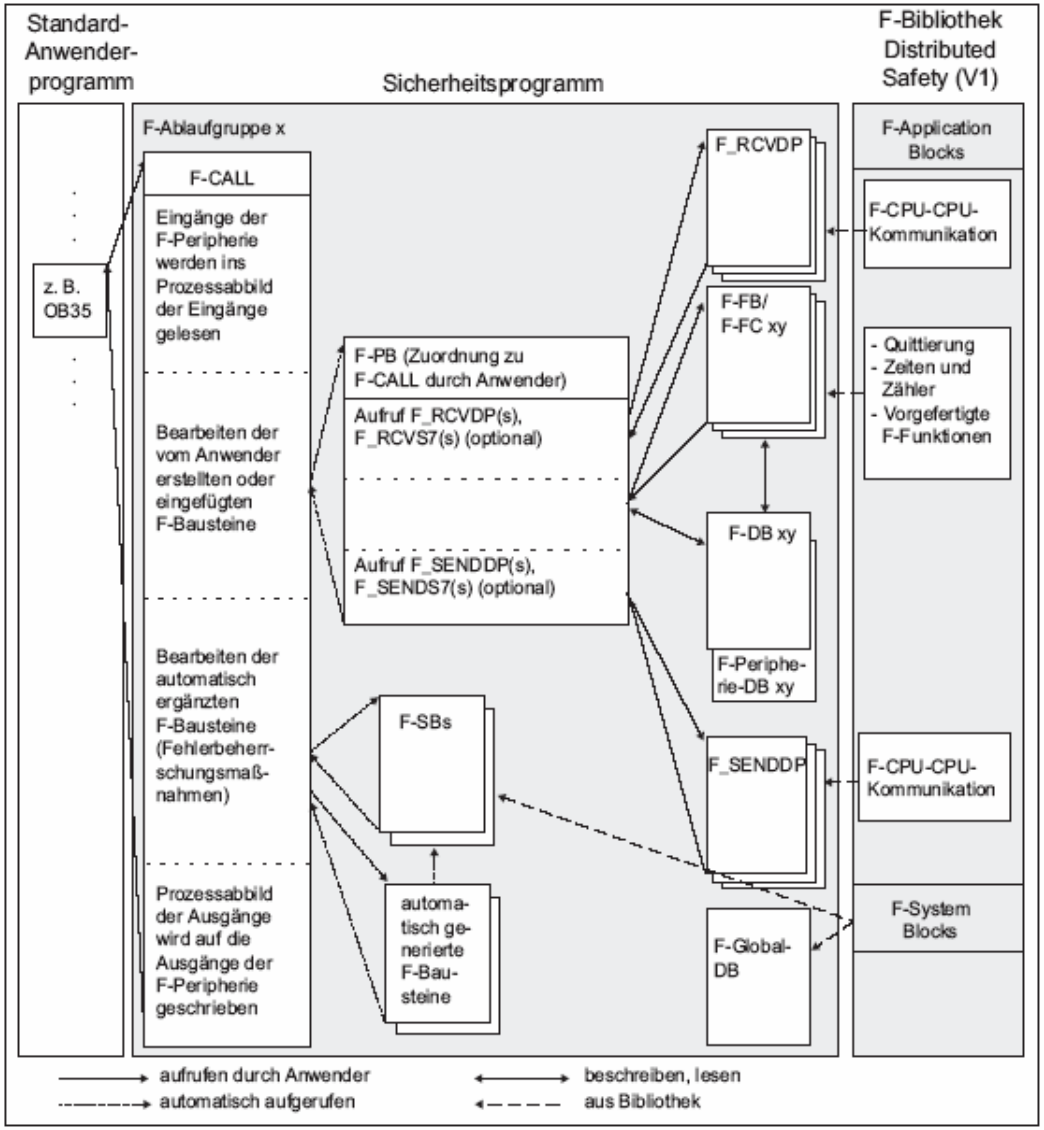
Michael Dziallas
ENGINEERING

5.1 Sicherheits- und Standard- Programm in einer CPU



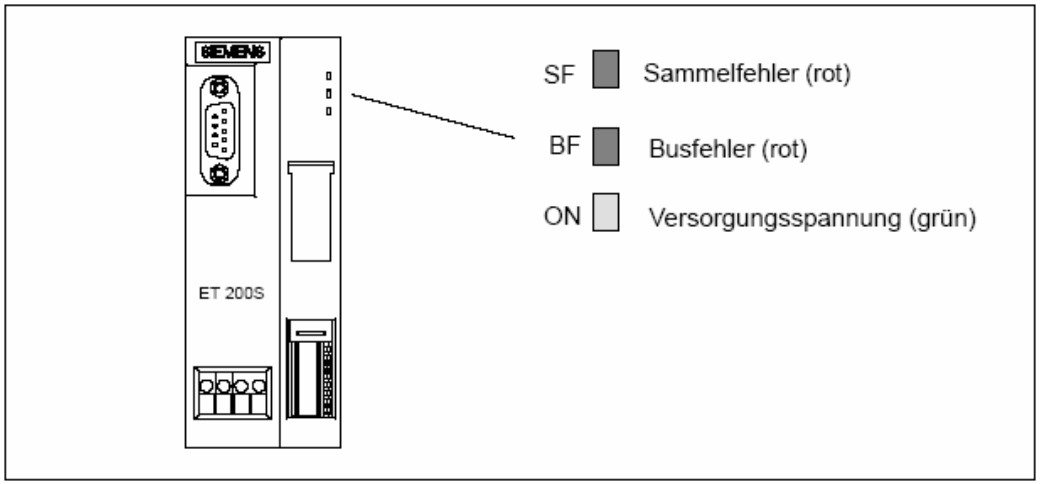
Michael Dziallas
ENGINEERING

5.2 Sicherheits- und Standard-Programm in einer CPU



Michael Dziallas
ENGINEERING

6.1 Diagnose LEDs der ET200S



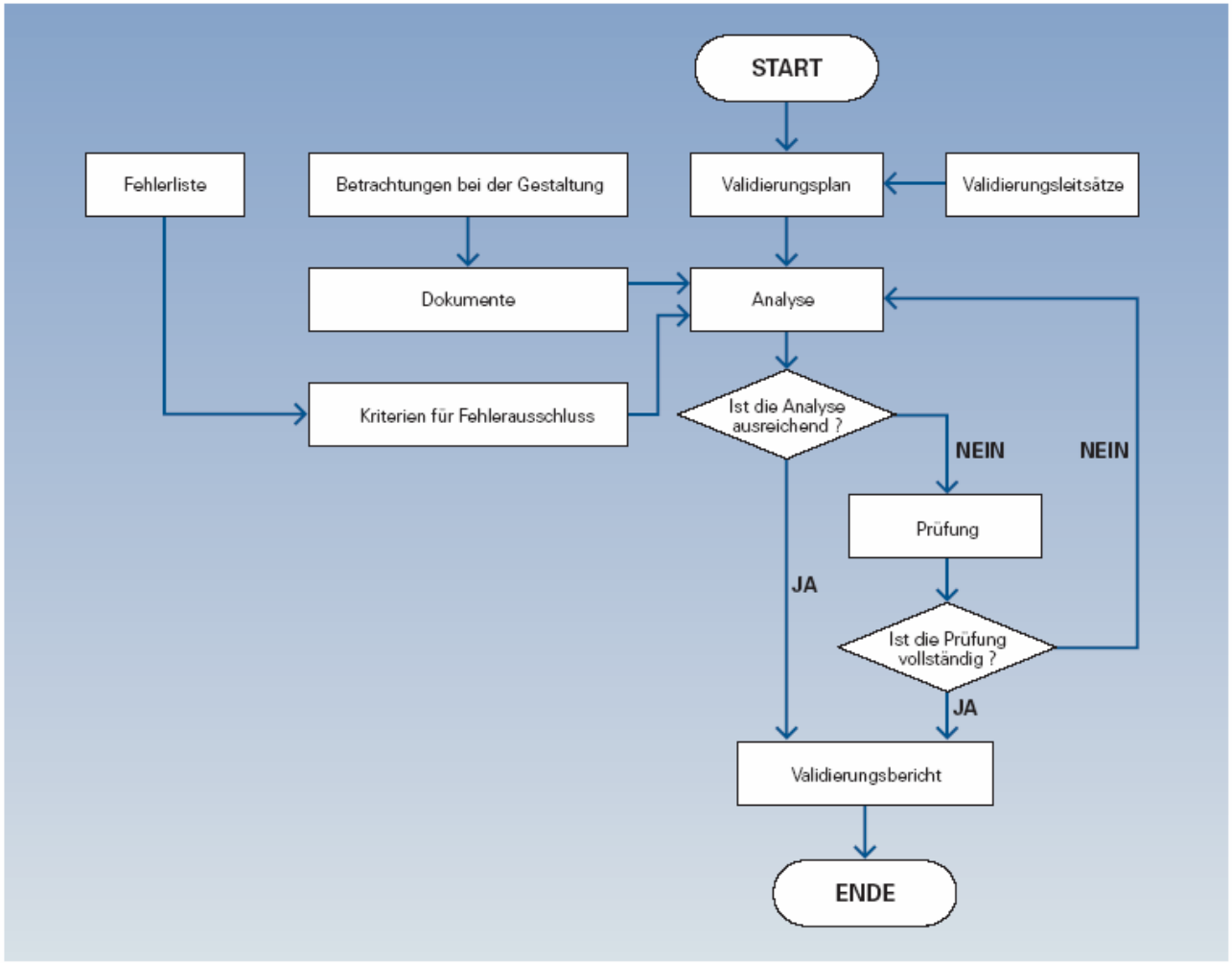
Michael Dziallas
ENGINEERING

6.2 Diagnosewerkzeuge

- **LEDs an der Hardware auswerten (F-CPU, F-Peripherie)**
- **Diagnosepuffer in *STEP 7* auswerten**
- **Stacks in *STEP 7* auswerten**
- **Diagnosevariable des F-Peripherie-DB über Test- und Inbetriebsetzungsfunktionen oder im Standard- Anwenderprogramm auswerten**
- **Diagnoseparameter der Instanz-DBs von F-Applikationsbausteinen über Test- und Inbetriebsetzungsfunktionen oder im Standard-Anwenderprogramm auswerten**

Michael Dziallas
ENGINEERING

9.1 Validierungsprozess



Michael Dziallas
ENGINEERING

9.1 Anforderung an die Dokumentation

Anforderungen an die Dokumentation	Kategorie, für die eine Dokumentation erfordlich ist				
	B	1	2	3	4
Grundlegende Sicherheitsprinzipien	X	X	X	X	X
Zu erwartende Betriebsbeanspruchungen	X	X	X	X	X
Einfluss des zu verarbeitenden Materials	X	X	X	X	X
Leistungsfähigkeit während anderer relevanter externer Einflüsse	X	X	X	X	X
Bewährte Bauteile	–	X	–	–	–
Bewährte Sicherheitsprinzipien	–	X	X	X	X
Das Prüfverfahren für die Sicherheitsfunktion(en)	–	–	X	–	–
Festgelegte Prüfintervalle	–	–	X	–	–
Bei der Gestaltung berücksichtigte, vorhersehbare Einzelfehler und das angewendete Erkennungsverfahren	–	–	X	X	X
Alle identifizierte Fehler gemeinsamer Ursache und wie sie verhindert werden	–	–	–	X	X
Wie die Sicherheitsfunktion bei jedem Fehler aufrechterhalten bleibt	–	–	–	X	X
Fehler, die zu erkennen sind	–	–	X	X	X
Verschiedene Fehleranhäufungen, die bei der Gestaltung zu berücksichtigen sind	–	–	–	X	X
Wie die Sicherheitsfunktion bei allen Fehlerkombinationen aufrechterhalten bleibt	–	–	–	–	X