

# INHALTSVERZEICHNIS

1. EINFÜHRUNG	1
1.1 Motivation	4
1.2 Übersicht	6
2. AUSWAHL DER FEHLERTOLERANZVERFAHREN	8
2.1 Ziele der Fehlertoleranz	10
2.1.1 Zuverlässigkeit	10
2.1.2 Sicherheit	11
2.1.3 Wirtschaftlichkeit	12
2.2 Bewertung von Fehlertoleranz	13
2.2.1 Gegenüberstellung der Begriffe und Kenngrößen	13
2.2.2 Geschlossene Darstellung der Fehlertoleranzkenngrößen	20
2.3 Klassenauswahl als Projektierungsverfahren für die Anwendung	21
2.3.1 Zuverlässigkeitsklassen für Tasks	22
2.3.2 Fehlertoleranzklassen für Funktionen	24
2.3.3 Auswahl einer Fehlertoleranzklasse	29
2.4 Realisierungsprinzipien	30
2.4.1 Industrielle Randbedingungen	30
2.4.2 Gliederung der Verfahren	32
2.4.3 Ausgewählte Verfahrenskombinationen	33
2.4.3.1 Klasse Z - Zuverlässigkeit	33
2.4.3.2 Klasse S - Sicherheit	35
2.4.3.3 Klasse W - Wirtschaftlichkeit	37
2.5 Gegenüberstellung ausgewählter Verfahren	39
3. DIE SYSTEM-HARDWARE	41
3.1 Die FIPS-Hardware-Struktur	41

3.1.1 Globale Grundstruktur dezentraler Automatisierungssysteme	42
3.1.2 Ergänzungen für die Fehlertoleranz	44
3.1.3 Systematische Gliederung und mögliche Ausbaustufen	46
3.1.3.1 Die Modulebene	46
3.1.3.2 Die Lokalsystemeebene	46
3.1.3.3 Die Regionalsystemeebene	47
3.1.3.4 Die Globalsystemeebene	49
3.2 Das Lokalsystem als Basissystem	51
3.2.1 Anforderungen der Fehlertoleranz an das Basissystem	51
3.2.2 Der Aufbau eines Lokalsystems	53
3.2.3 Die Baugruppen des Basissystems	56
3.2.3.1 Der Mikrorechner (MIC)	56
3.2.3.2 Die Speicherbaugruppe (M)	58
3.2.3.3 Das Konsolen-Interface (CI)	60
3.2.3.4 Die Analog-Ein/Ausgabe (AIO)	63
3.2.3.5 Die Binär-Ein/Ausgabe (BIO)	66
3.2.3.6 Der Globalbuskoppler (GBC)	68
3.2.3.7 Die Stromversorgung (PS)	68
3.3 Der Regionalbus als zusätzlicher Kommunikationsweg	71
3.3.1 Anforderungen an einen Kommunikationsweg	71
3.3.2 Das Prinzip des Regionalbus	72
3.3.3 Der Aufbau eines Regionalbuskopplers	73
3.3.4 Die wichtigsten Funktionen der Regionalbuskoppler	76
3.3.5 Die Nutzung für die Fehlertoleranz	79
3.4 Die Realisierung dezentraler Voter	83
3.4.1 Anforderungen an dezentrale Voter	84
3.4.2 Die Anordnung für hohe Zuverlässigkeit	85
3.4.3 Die Anordnung für sicherheitsgerichtetes Verhalten	87
3.4.4 Die Bedeutung des Schaltelements	89
3.4.5 Ein Implementierungsbeispiel	92
3.5 Die realisierte System-Hardware	94
3.5.1 Die Aufbautechnik	94
3.5.2 Der Umfang des aufgebauten Systems	94

4. DIE SYSTEM-SOFTWARE	99
4.1 Die Anforderungen an das Betriebssystem	102
4.1.1 Randbedingungen in der Automatisierungstechnik	102
4.1.2 Spezielle Anforderungen durch die Fehlertoleranz	103
4.2 Das Betriebssystem REX im Überblick	106
4.2.1 Die Systemphilosophie	106
4.2.2 Behandelte Objekte	108
4.2.3 Schichten und Oberflächen	109
4.3 Die dezentrale Datenhaltung	115
4.3.1 Die Segmentierung von Anwenderprogrammen	116
4.3.2 Regional zugängliche System-Informationen	119
4.3.3 Die Lokalsystembeschreibung	122
4.4 Die Koppel-Software	124
4.4.1 Die Funktionen der Koppel-Software	124
4.4.2 Ein Beispiel für die regionale Ausführung eines Systemaufrufs	127
4.5 Die Exekutive	129
4.5.1 Die Hierarchie in der Exekutive	129
4.5.2 Die Bearbeitung von Jobs und Tasks	131
4.5.2.1 Die unbewußten Exekutivzustände	132
4.5.2.2 Die bewußten Funktionszustände	138
4.5.3 Kommunikationsmittel für Jobs und Tasks	142
4.5.3.1 Direkte Kommunikation	143
4.5.3.2 Botschaftenorientierte Kommunikation	143
4.5.4 Die Prozeß-Ein/Ausgabe	146
4.5.4.1 Die analoge Eingabe als Beispiel	147
4.5.5 Eine Übersicht über Systemaufrufe	148
4.6 Der Konfigurator	159
4.6.1 Der Systemstart	160
4.7 Das Dialogsystem	163
4.7.1 Die Schnittstelle zum Anwenderprogramm	164
4.7.2 Die Bedienfunktion	165
4.8 Die Bibliothek	169
4.9 Die Realisierung des Betriebssystems	171

5. SPEZIELLE ENTWICKLUNGSHILFEN	174
5.1 Hilfsdateien für die Erstellung einer Task	174
5.2 Bibliotheken und zugehörige Extern-Deklarationen	177
6. FEHLERTOLERANTE REGELPROGRAMME	180
6.1 Digitale Regler in verschiedenen Fehlertoleranz- klassen	180
6.1.1 Die Software-Realisierung der Regler	183
6.1.1.1 Rekonfigurierbare Regler der Klasse W	184
6.1.1.2 Sicherheitsgerichtete Regler der Klasse S	187
6.1.1.3 Hochzuverlässige Regler der Klasse Z	190
6.1.2 Experimente an analog simulierten Prozessen	192
6.1.2.1 Die Erzeugung von Fehlern	192
6.1.2.2 Die Versuchsanordnung	193
6.1.2.3 Ein Beispielexperiment	195
6.2 Fehlertolerierende, schnelle adaptive Mehrgrößen- regelung	200
6.2.1 Der parameteradaptive Regelkreis	201
6.2.2 Die Elemente des parameteradaptiven Regelkreises	202
6.2.3 Die Realisierung in der Fehlertoleranz- klasse W	206
7. GEGENÜBERSTELLUNG DER FEHLERTOLERANZKLASSEN	212
7.1 Die tolerierbaren Fehler	212
7.2 Die Verbesserung relevanter Kenngrößen	216
7.3 Der erforderliche Aufwand	221
8. ZUSAMMENFASSUNG	226
LITERATURVERZEICHNIS	229
ANHANG	239