Qualitätssicherung für moderne Systeme

Autor(en): **Lanz, Otto E.**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **83 (1992)**

Heft 19

PDF erstellt am: **29.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-902879

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Qualitätssicherung für moderne Systeme

Otto E. Lanz

Es wird gezeigt, wie eine sinnvolle, ausreichende und wirtschaftlich vertretbare Typenprüfung von Geräten und Systemen mit variablen Hard- und Software-Modulen durchgeführt werden kann. Voraussetzung ist, dass die Hard- und Software nach fehlereinschränkenden Regeln und Verfahren entwickelt wird und durch formale Methoden übersichtlich gemacht werden kann. Dazu gehört auch ein funktionierendes internes Qualitätssystem mit entsprechender Dokumentation, Spezifikationen und Weisungen, die auditiert werden können.

L'article montre comment un essai de type judicieux, suffisant et économiquement justifié d'appareils et systèmes peut être réalisé avec des modules de matériels et logiciels variables. Pour cela, il faut que le matériel et le logiciel ont été développés selon des règles et méthodes à limitation d'erreurs et peuvent être rendus transparents grâce à des méthodes formelles. En fait partie un système interne d'assurance de la qualité disposant d'une documentation, spécifications et directives appropriées qui peuvent faire l'objet d'un audit.

Adresse des Autors
Dr. *Otto E. Lanz*, Geschäftsleiter, ABB Relays AG, 5401 Baden.

Problemstellung

Qualitätssicherung für Geräte und Systeme mit softwareabhängiger Funktionalität

Moderne Geräte und Systeme für Schutz- und Stationsleittechnik sind in ihrer Funktionalität zunehmend durch Software bestimmt. Die Hardware ist so strukturiert, dass die einzelnen Module den folgenden Hauptaufgaben entsprechen (siehe Bild 1):

a) Erfassung und Aufbereitung der Analogwerte (Strom/Spannung)
b) Bearbeitung der Algorithmen (zum Beispiel Schutzfunktionen)
c) Verarbeitung der Logiksignale
d) binäre Ein- und Ausgaben
e) Kommunikation, Datenaustausch mit anderen Geräten, lokale Bedienung, dezentrale Datenbank.

Diese Module sind untereinander in der Regel über eine Busstruktur verbunden. Der Hardware ist eine Software-Struktur überlagert, deren Elemente (Module) teilweise oder ganz auf die Hardware-Module aufgeteilt sind (siehe Bild 2). Veränderungen der Funktionen können sowohl durch die Auswahl der Hardware als auch durch die Auswahl von Software-Modulen bewerkstelligt werden. So stehen zum Beispiel bei den Geräten REG 216 und REL 316 von ABB Relays eine Vielzahl (>35) von Software-Modulen in Form einer Funk-

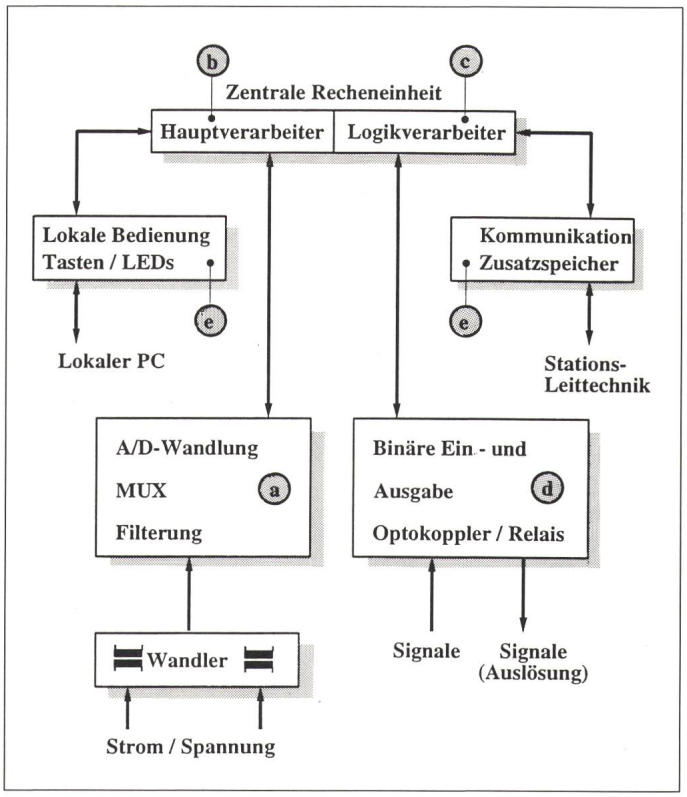

Bild 1
Hardware-Struktur
a Erfassung und Aufbereitung der Analogwerte
b Bearbeitung der Algorithmen (zum Beispiel Schutzfunktionen)
c Verarbeitung der Logiksignale
d binäre Ein- und Ausgabe
e Kommunikation, Datenaustausch, lokale Bedienung

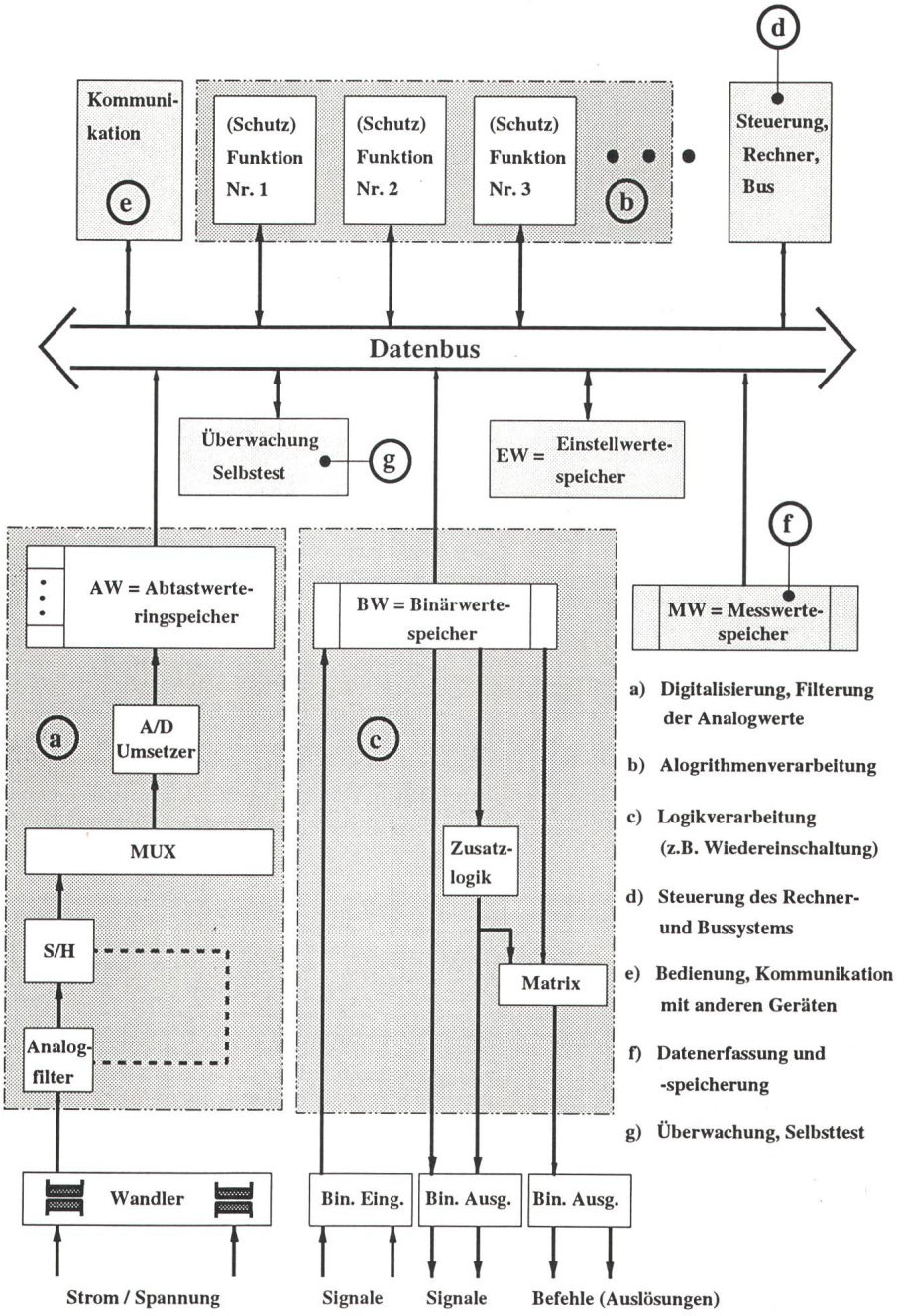

Bild 2 Software-Struktur

tionsbibliothek zur Verfügung. Damit lassen sich für einzelne Anwendungsbereiche entsprechende Pakete zusammenstellen. Diese gestatten es dem Anwender, in optimaler Weise den Anforderungen der Schutzobjekte Rechnung zu tragen. Aus diesen Geräten wiederum lassen sich modulare und vollständig dezentralisierte Stationsleitsysteme mit koordiniertem Schutz zusammenstellen, welche untereinander und mit einer zentralen Stationseinheit (MMK, zentrale Datenbank, zentrale Funktionen, Fernwirkanschluss) mit einem seriellen Lichtleiterbus verbunden sind. So erhält der Anwender eine optimale Lösung für die Anforderungen der Sekundärtechnik in seiner Station. Die Systemfunktionalität ist wieder weitgehend durch Software-Funktionen bestimmt.

Die Frage der Prüfbarkeit

Aufgrund der oben dargelegten Anpassung der Funktionalität stellen sich natürlich für Hersteller und Anwender neue Fragen in bezug auf die Prüfbarkeit und somit der Relevanz von Typenprüfungen. Dies betrifft im besonderen die enorme Vielfalt, die sich durch mögliche Kombinationen von Hardware- und Software-Modulen ergeben. Allein die Kombination von 5 verschiedenen Modulen ergibt 31 Varianten, wenn man die Reihenfolge und die verschiedenen Einstellmöglichkeiten (Parameter) nicht berücksichtigt. Bei 10 Modulen sind es bereits über 1000 Varianten.

Im folgenden wird aufgezeigt, wie im Rahmen der Qualitätssicherung sichergestellt werden kann, dass trotz der enormen Kombinationsmöglichkeiten durch die Auswahl einzelner Module eine hohe Sicherheit und Verlässlichkeit der Schutz- und Stationsleittechnik Funktionen gewährleistet werden kann.

Typenprüfung

Die Typenprüfung einer Funktion, eines Gerätes oder eines Systems ist der abschliessende Nachweis des Herstellers der dem Kunden garantierten Daten und Fähigkeiten. Die Typenprüfung wird an einer Hardware und Software ausgeführt, die nach den Richtlinien und Unterlagen der Entwicklung, Konstruktion und Fabrikation normal gefertigt wurde. Um eine Typenprüfung in diesem Sinne durchzuführen und ihre Ergebnisse für alle Kunden akzeptabel werden zu lassen, sind im wesentlichen zwei Dinge notwendig:

- eine Spezifikation für die Typenprüfung
- Normen (international anerkannte).

Die Spezifikation für die Typenprüfung legt den Ablauf fest und bestimmt, welche Regeln eingehalten werden müssen. Sie besagt wie und was geprüft wird, welche Grundsätze für die Überprüfung der Ergebnisse angewandt werden (Instrumente, Genauigkeiten, Checklisten usw.) und welche Dokumente schliesslich zu erstellen sind.

Die Anforderungen für die Prüfung stammen hauptsächlich aus den Erfordernissen der Anwendung des zu prüfenden Objektes. Meist ist das ein Pflichtenheft für ein Gerät oder ein System, beziehungsweise das entsprechende Datenblatt. Andererseits sind die Anforderungen, die die Einflüsse aus der Umgebung betreffen, in der das Objekt seine Funktionen ausüben muss, in international anerkannten Normen festgelegt.

Inhalt der Typenprüfung

Eine umfassende Typenprüfung eines Gerätes oder eines Systems be-

inhaltet im allgemeinen folgende Hauptpunkte:

- visuelle Kontrolle, Dokumentation
- statische Funktionsprüfung
- dynamische Funktionsprüfung
- Tests zum Nachweis der Unabhängigkeit der Funktion von der Betriebsumgebung (zum Beispiel Temperatur, Feuchtigkeit usw.)
- Isolationsprüfungen
- EMV-Tests (Prüfung der Sicherheit gegenüber elektrischen Störungen)
- Beeinflussung durch die elektrische Speisung
- elektrische Verbrauchsmessungen
- Kontrolle der Kontaktbelastungen
- Prüfung der mechanischen Festigkeit
- zusätzliche Spezialprüfungen (je nach Objekt).

Die nebenstehende Tabelle (siehe Rahmen) zeigt eine Übersicht über die wichtigsten Normen, die heute im Bereich Schutz- und Stationsleittechnik von Bedeutung sind.

Das bisherige Verfahren für Typenprüfungen ist primär auf Hardware ausgerichtet. Der Aufwand für eine umfassende Typenprüfung kann sehr gross sein. So sind zum Beispiel bei der Prüfung eines Distanzschutzes allein schon für die statischen und dynamischen Funktionstests sowie die Abhängigkeitstests für die Betriebsumgebung (zum Beispiel Temperatur) nach den Richtlinien der Cigré rund 1800 einzelne Prüfungen notwendig.

Betrachtet man nun Geräte, die Software enthalten, so ist das Verfahren der Typenprüfung wie bisher anwendbar, solange die Software als integraler Bestandteil des Gerätes und seiner Funktion angesehen werden kann (sogenannte Firmware). Bei Geräten und Systemen, die mehrere vom Anwender aktivierbare und konfigurierbare Software-Module enthalten, ergeben sich neue Gesichtspunkte bezüglich der Vorgehensweise für die Prüfungen. Dabei ist das Vorgehen in der Entwicklungsphase als auch während der Typenprüfung zu betrachten.

Prüfungsformen	Prüfgrössen	Normen
Thermische und elektrische Prüfungen		
Temperatur- und Klimaprüfung	Kälte 16 Std. Wärme trocken Feuchte Wärme	IEC 68-2-1 IEC 68-2-2 IEC 68-2-3
Kurzunterbrechung der Hilfsspannung	0...50 ms	IEC 255-11, VDE 0435 Teil 303
Belastbarkeit der Eingänge (Spannung/ Strom)	Spannung 1,2 oder 2 U_N 1,1 U_N 10 s Strom 2/4 I_N 30 I_N 10 s 100 I_N 1 s 250 I_N peak	 VDE 0435 Teil 303 IEC 255-3/-4 IEC 255-3, VDE 0435 Teil 303 IEC 255-3/-4,VDE 0435 Teil 303 IEC 255-3/-4,VDE 0435 Teil 303
Isolationswiderstand	0,5 kV DC	IEC 255-5, VDE 0411 Kl. 1
Isolationsspannung	2 kV AC 1 min	IEC 255-4/-5, VDE 0160 Kl. 4, VDE 0411 Kl.1,VDE 0435 Teil 303 Kl. C, BS 142-1966 ANSI/IEEE C37.90-1978
Stossspannung	1,2/50 us Kl. 1 / 2 / 3	 IEC 255-4/-5, VDE 0110 Kl. C, VDE 0432, VDE 0435 Teil 303
Elektromagnetische Verträglichkeit (EMV)		
1 MHz burst disturbance test	1 MHz 400 Hz Kl. 1/2/3 0/0; 0,5/1; 1/2,5 kV	 IEC 255-22-1 (1988), VDE 0435 Teil 303, ANSI/IEEE C37.90.1-198x
Electrostatic discharge test (ESD)	Kl. 1/2/3/4 2/4/8/15 kV	 IEC 255-22-2 (1989), IEC 801-2
Radio frequency interference test (Walkie Talkie)	80, 160, 460 MHz Kl. 1/2/3 1/3/10 V/m	 IEC 255-22-3 (1989), IEC 801-3
Fast transient test	Kl. 1/2/3/4 0,5/1/2/4 kV	 IEC 255-? (in Bearbeitung) IEC 41B Sec. (64), IEC 801-4
Mechanische Prüfungen		
Resonanzermittlung/ Vibrationsprüfung	1–100 (150) Hz 1g (2 g)	 IEC 255-21-1, IEEE 344-1987
Erdbebenprüfung	1–35 Hz 1–5 g	IEC 255-21-2, IEEE 344-1987

Entwicklung und Prüfung der Software

Hauptsächliche Module der Software

Geräte und Systeme für Schutz und Stationsleittechnik, deren Funktionalität zu einem wesentlichen Teil durch Software-Module bestimmt ist, beinhalten in der Regel folgende Module (siehe Bild 2):

a) Digitalisierung und Filterung der Analogwerte
b) Algorithmenverarbeitung (Schutzfunktionen, ...)
c) Logikverarbeitung (Auslöselogik, Wiedereinschaltung, ...), Prozess-Steuerung (überwachte Befehlsausgabe, ...), Prozess-Überwachung (Stellungsmeldungen, Gasdichten, ...), Verriegelungen und Automatiken
d) Steuerung des Rechner- und Bussystems
e) Bedienung (MMK) und Kommunikation mit externen Geräten (Fernwirken)
f) Datenerfassung und -speicherung (Störwertaufzeichnung)
g) Überwachung, Selbsttest.

Jedes dieser Module hat eine oder mehrere Schnittstellen zu anderen

Modulen. Daraus ist ersichtlich, dass mehrere Schutzfunktionen auf dieselben Daten (zum Beispiel Messwerte von Strom und Spannung) Zugriff haben. Ferner werden verschiedene Funktionen von einer zentralen Steuerung wahrgenommen. Die Logikverarbeitung und damit Auslösung und/oder Signalisierung werden ebenfalls von verschiedenen Funktionen angesteuert. Das Zusammenwirken ist somit durch die gewählte Konfiguration der Hard- und Software bestimmt.

Dieser Sachverhalt des Zusammenwirkens ist grundsätzlich gleich wie bei hardwarebasierten Systemen. Entsprechende Entwurfs- und Konstruktionsregeln (Kontaktbelastungen, Drahtquerschnitte usw.) sorgen für ein möglichst rückwirkungsfreies Zusammenspiel. Im gleichen Sinn, aber angepasst auf die Erstellung der Software, wird für ein einwandfreies Funktionieren der unterschiedlichen Kombinationen von Hard- und Software gesorgt.

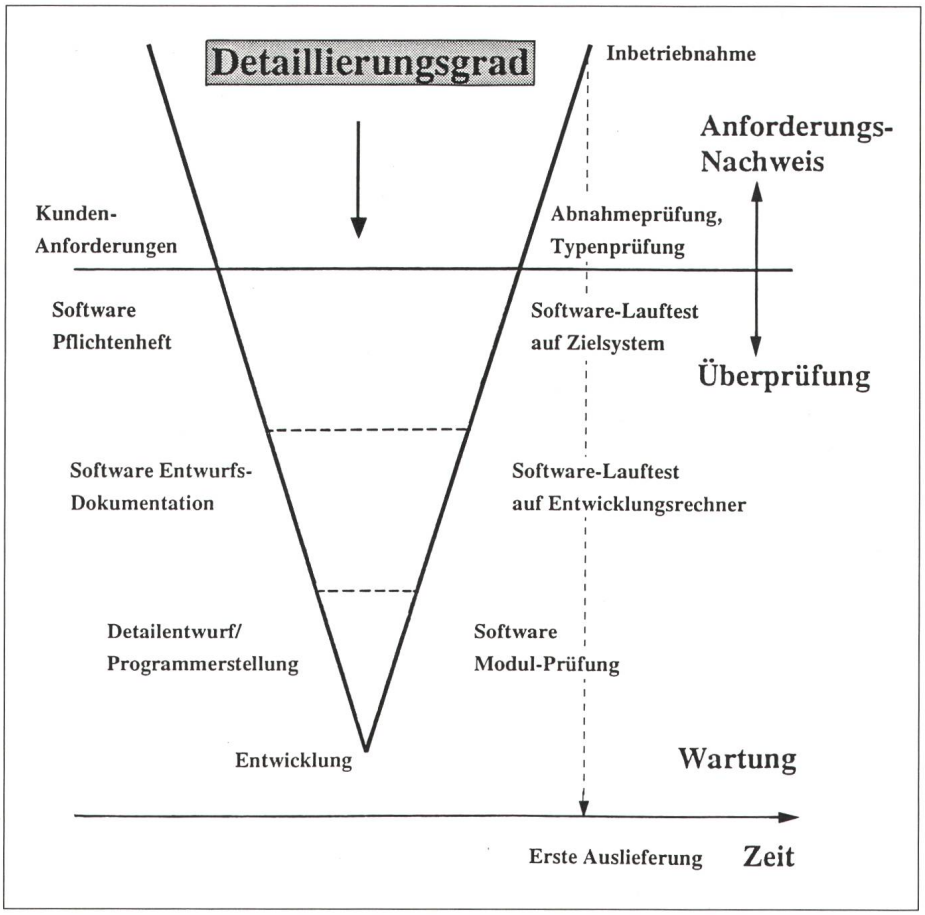

Bild 4 Prüfmethodik

Entwicklung von Software

Um eine Alles-und-Jedes-mit-Jedem-Prüfung zu vermeiden, muss die Software nach bestimmten Richtlinien und Kriterien entwickelt werden. Die Prüfung ist abhängig von den Entwurfsregeln, dem Aufbau und den Schnittstellen der Software. Um ein Programm als Ganzes oder als Teil überprüfbar zu machen, muss es möglichst *klar überschaubar*, möglichst *in sich geschlossen* sein und *wenige, aber klar definierte Schnittstellen* nach Aussen aufweisen. In Bild 3 ist eine typische Programmstruktur dargestellt. Sowohl der Signalfluss als auch die Interaktion mit den entsprechenden Speichern ist daraus ersichtlich. Allgemein bewährte Methoden, die bei der Entwicklung von Geräten und Systemen beispielsweise bei ABB Relays AG berücksichtigt werden, sind:

- strukturiert programmieren (Sprache)
- Entwurf von oben nach unten, schrittweise Verfeinerung
- Verwendung von Case-Tools (Computergestützte Werkzeuge für Software-Entwicklung)
- Entwurf und Überprüfung durch Simulation.

Im Detail sind vor allem die möglichen Abhängigkeiten eines Programmes zu beachten, zum Beispiel von:

- internen Abläufen
- der Rechnerleistung
- Kommunikationsprotokollen
- Datenquellen
- Hilfsprogrammen (zum Beispiel Selbstüberwachung).

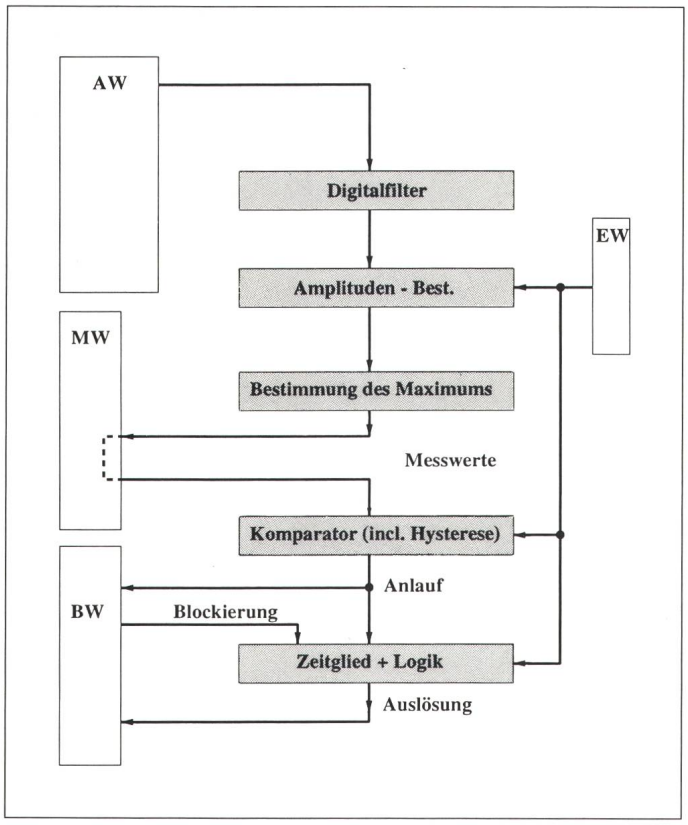

Bild 3
Ablauf einer Schutzfunktion
AW Abtastwertespeicher
BW Binärwertespeicher
EW Einstellwertespeicher
MW Messwertespeicher

Um die erwähnten Anforderungen an die Software-Entwicklung in den Griff zu bekommen und international zu regeln, sind die IEC-Empfehlungen 65A ausgearbeitet worden. Hier werden neben Regeln für den Entwurf, Überprüfung und Validation auch Anforderungsklassen eingeführt.

Prüfung von Software

Als Verfahren für die Prüfungen wird ein Von-unten-nach-oben-Modell angegeben (siehe Bild 4). Ausgehend von den Kundenanforderungen nimmt die Prüftiefe (Detaillierungsgrad) im Laufe der Zeit zu und erreicht in der Phase der Entwicklung ein Maximum. Anschliessend findet ein Übergang zur Abnahme- und Typenprüfung, mit schrittweiser Reduktion der Prüftiefe, statt. In diesem Modell erscheint auch die Typenprüfung als letzte Stufe vor der Inbetriebnahme der Geräte und Systeme.

IEC 65A verlangt unter Abschnitt 14 für die Software-Validation:

- Wahrscheinlichkeitstest
- Modell /Simulation
- Funktions- und Blackbox-Prüfungen.

Die Prüfungen auf Fehlerwahrscheinlichkeit werden wegen des hohen Aufwandes nur für hohe und höchste Sicherheitsklassen empfohlen. Es ist angezeigt, solche Tests in vernünftigem Mass mit in die Funktionsprüfungen einzubeziehen. Unter Modell/Simulation werden formale Methoden angegeben, die es erlauben, die Struktur der Software in bezug auf die oben erwähnten Abhängigkeiten offenzulegen. Dieser Punkt ist sehr interessant, da auch hier dahinter steht, dass ein folgender Funktionstest nur erfolgreich aber auch aufwandsgerecht durchgeführt werden kann, wenn das Programm(teil) formal auf eine korrekte Struktur überprüft wurde. Für die Funktions- und Blackbox-Prüfungen werden als wichtigste Methoden empfohlen:

- Grenzwert-Analyse (zum Beispiel Extremwerte für Einstellwerte)
- Ähnlichkeitsklassen-Prüfung (zum Beispiel Einteilung der Einstellwerte in ähnliche Gruppen)
- Prozess-Simulation.

Zu ähnlichen Empfehlungen gelangt auch TC7 des «European Workshop on Industrial Computer Systems» in seinem Papier über «Techniques for Verification and Validation of Safety Related Software». Hier ist die Wahl der Methoden nur noch weniger vorgegeben.

Praktische Prüfung der Software

Durchführung

Wir unterscheiden zwei Stufen für die Prüfung von Software.

a) *Hardware-Prüfung mit vollständig installierter Software:* Hier geht es darum, bei einem neuen Gerät oder System zuerst die Typenprüfung der Hardware durchzuführen. Dabei sind folgende Punkte zu beachten:

- Implementierung der Software in der Maximalkonfiguration und möglichst 100%iger Auslastung des Rechners (oder der Rechner).
- Vorprüfung, welche das korrekte Einstellen der Parameter (Bedienung, MMK) und grundlegende Überprüfung der geladenen Funktionen inkl. binäre Ausgaben (Start- und Tripsignale) umfasst.
- Anschliessende Hauptüberprüfung des Gerätes auf alle Umwelteinflüsse (Temperatur, Klima, EMV, mechanische Festigkeit, Speisungsabhängigkeit usw.) gemäss den entsprechenden Normen. Dabei werden ein bis drei Funktionen an den Ansprechgrenzen im spezifizierten Toleranzbereich überwacht. Die übrigen Funktionen werden auf korrekte Signalisierung kontrolliert.

Die Prüfung gilt besonders der Hardware. Aber auch die System-Software des Gerätes (mit einer ersten Funktionsüberprüfung), der Datenzugriff und die Algorithmenverarbeitung werden dabei auf korrektes Verhalten überprüft. Wird dieser Teil bestanden, kann man davon ausgehen, dass die Hardware mit ihrer System-Software in Ordnung ist.

b) *Software-Funktionen:* Im zweiten Teil der Prüfung wird der Rechner wieder voll ausgelastet. Dabei wird eine Funktion nach der anderen (wobei stets alle aktiv sind) schrittweise und sehr detailliert überprüft. Das Gerät oder das System wird dabei unter Referenzbedingungen betrieben.

1. Schritt: Prüfung der Bedienung (MMK)
- Menüdurchlauf, Verzweigungen, Rücksprünge
- Werteinstellungen (Parameter), Übernahmekontrollen
- Rückmeldungen, Ausgabe.

Diese Kontrolle wird Funktion für Funktion wiederholt, vor allem mit Grenzwerten für die Einstellwerte.

2. Schritt: Der zweite Schritt enthält die Funktionsprüfung mit statischen, dynamischen und Abhängigkeitsmessungen (zum Beispiel Ansprechwert als Funktion der Temperatur oder der Speisespannung). Hier kommen alle in IEC 65A unter «Functional and Blackbox Testing» genannten Methoden zur Anwendung. Nach der Struktur in Bild 2 werden damit die (Software-)Module, zum Beispiel Algorithmenverarbeitung, Abtastwertspeicher, Einstellwertspeicher und die jeweilige Verwendung der richtigen Daten für die entsprechende Funktion sowie die korrekte Zuordnung der Ergebnisse überprüft. Ferner wird der interne Ablauf und die Logik der einzelnen Funktionen verifiziert (siehe Bild 3).

3. Schritt: Der dritte Schritt befasst sich mit externer Kommunikation.
- Datenaustausch in verschiedenen Betriebsfällen
- Wertübergabe bei aktiver Funktion
- «Timeout»-Tests bei maximalem Anfall von Daten (Überprüfung auf Hängenbleiben).

4. Schritt: Dieser befasst sich im Zusammenhang mit der Bedienung (MMK) und externer Kommunikation mit Erfassung, Speicherung und Ausgabe von Zusatzdaten wie:
- Messwerten
- Ereignissen
- Daten (zum Beispiel für Störschreiber).

Diese werden wieder wechselweise mit der Aktivierung verschiedener Funktionen getestet.

5. Schritt: Hier sind gemäss Bild 2 noch der Binärwertespeicher und die Zusatzlogik intensiver zu testen. Jede Schutz- und Stationsleittechnik-Funktion liest und verarbeitet Binärwerte und beeinflusst umgekehrt mit solchen Werten die Logik. Dabei ist es praktisch unmöglich, alle Kombinationen durchzuprüfen. So müssen mit Zufallsgeneratoren willkürliche Kombinationen von aktiven Eingängen erzeugt und entsprechende Betriebsfälle simuliert werden. Eine zweite Methode bezieht sich auf die gegebene Funktionsstruktur und die bekannten Anforderungen, um gezielte Simula-

tionen durchzuführen, zum Beispiel standardisierte HF-Logik für Distanzschutz.

6. Schritt: Für die Steuerung sind die Eingänge, mit einem Schaltersimulationsgerät verbunden, zu testen. Dabei wird die Funktion der Stellungsmeldungserfassung/-überwachung und die überwachte Befehlsausgabe einschliesslich der lokalen Verriegelung getestet.

7. Schritt: Zum Test eines gesamten SCS mit/ohne koordinierten Schutz ist das System mit seiner Kommunikation vollständig oder teilweise aufzubauen. Damit wird dann sowohl die sichere Funktion der übergeordneten Verriegelung als auch die vollständige Verarbeitung von simulierten Ereignis- und Alarmlawinen nachgewiesen.

Änderung von Hardware und Software

Für jeden Anwender ist die Frage interessant, was geschieht, wenn Änderungen und Ergänzungen an Hardware und/oder Software vorgenommen werden.

Änderungen: Wenn wir von Bild 2 ausgehen und zum Beispiel eine geänderte Zusatzlogik annehmen, dann ist klar, dass zum Beispiel die Verarbeitung der Analogwerte, der Messwertespeicher, die System-Software und die Bedienung (MMK) nicht involviert sind. Direkt betroffen sind die Zusatzlogik und der Binärwertespeicher. Bedingt betroffen sind die Schutzfunktionen. In ihnen ändert sich zwar nichts, es könnte aber durch einen Fehler in der Zusatzlogik eine falsche Situation vorgetäuscht werden. Wie ausführlich die Prüfung nach Schritt 5 wiederholt werden muss, ist wieder von der formalen Analyse des Programmteiles und der Änderung abhängig und muss damit für jeden einzelnen Fall separat entschieden werden. Wird beispielsweise die System-Software geändert, so ist die Typenprüfung nach obigem Abschnitt a) «Hardware-Prüfung mit vollständig installierter Software» und für entsprechende Teile von Abschnitt b) «Software-Funktionen» zu wiederholen.

Erweiterung durch eine neue oder geänderte Funktion: Wird die Bibliothek der Schutz- und Steuerungsfunktionen um eine neue oder geänderte erweitert, sind für diese Funktion alle Prüfungen gemäss obigem Schritt 2 durchzuführen. Die Prüfung der Zusatzlogik ist nach den oben genannten Kriterien zu ergänzen. Für die anderen Funktionen (zum Beispiel MMK) sind wegen Ablaufkontrolle, Rechnerkapazität und Datenabhängigkeit Stichprobenprüfungen zu machen. Die Erfahrung hat hier gezeigt, dass aufgrund der eingehaltenen Entwurfsregeln nie Beeinflussungen aufgetreten sind.

Variation der Bibliotheksfunktionen: Werden geprüfte Funktionen in einer Bibliothek vervielfältigt oder ausgetauscht, besteht ausser der Kontrolle der Rechner-Auslastung aufgrund der Strukturen in Bild 1 und Bild 2 kein Grund für eine Nachprüfung.

Andere Hardware: Die Hardware-Konfiguration kann durch die Anzahl der Module variiert werden (zum Beispiel mehrere Rechner und/oder Ein-/Ausgabeeinheiten). Voraussetzung ist, dass diese Hardware mit entsprechender Software nach obigem Abschnitt a) «Hardware-Prüfung mit vollständig installierter Software» typengeprüft ist. Die Hardware hat aber grundsätzlich die gleiche Architektur mit gleicher System- und Datenverarbeitungs-Software.

Für eine erste Betrachtung ist wieder die Auslastung der gesamten Rechner-Kapazität wichtig. Die Zusatzlogik muss neu geprüft werden, wenn durch weitere Ein-/Ausgabemodule ihre Funktion erweitert wird. Unter Umständen kann neben der Zusatzlogik auch die Bedienung verschieden sein. Wird nun eine Schutzfunktion, die auf einer ähnlichen Hardware-Konfiguration geprüft wurde, übernommen, so muss nicht die interne Struktur des Programms dieser Funktion neu überprüft werden, sondern die Schnittstellen zu der neuen Umgebung. Das bedeutet:

- ausführliche Prüfung der Bedienung und der Kommunikation
- Grenzwertüberprüfungen (Einstellwerte)
- Zeitverhalten
- Messwerte, Daten für Störwerterfassung
- Überprüfung der Logik.

Eine Wiederholung der gesamten Typenprüfung wäre nicht sinnvoll und stünde in keinem vernünftigen Verhältnis zum erforderlichen Aufwand.

Zusammenfassung

Zusammenfassend kann festgestellt werden, dass eine sinnvolle, ausreichende und auch wirtschaftlich vertretbare Typenprüfung von Geräten und Systemen mit variablen Hard- und Software-Modulen durchgeführt werden kann. Voraussetzung ist, dass die Hard- und Software nach fehlereinschränkenden Regeln und Verfahren entwickelt wird und durch formale Methoden weitgehend übersichtlich gemacht werden kann. Dazu gehört allerdings ein funktionierendes internes Qualitätssystem, mit entsprechender Dokumentation, Spezifikationen und Weisungen, die auch auditiert werden können. Von ABB Relays AG sind Tausende von Geräten, deren Funktionalität sehr wesentlich durch Software bestimmt ist, seit mehreren Jahren erfolgreich im Einsatz. Die von den Kunden gemachten Betriebserfahrungen haben die Richtigkeit des beschriebenen Vorgehens in bezug auf Prüfung der Hard- und Software bestätigt.

Anmerkung: Dieser Aufsatz ging aus einem Referat hervor, welches anlässlich der ETG-Tagung vom 7. Mai 1992 in Baden gehalten wurde.