**Zeitschrift:** Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

**Herausgeber:** Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

**Band:** 78 (1987)

**Heft:** 7

**Artikel:** Busorientierte digitale Leittechnik in Kernkraftanlagen

**Autor:** Salm, M.

**DOI:** https://doi.org/10.5169/seals-903849

# Busorientierte digitale Leittechnik in Kernkraftanlagen

M. Salm

***Dieser Beitrag begründet die konservative Praxis bei der Bewilligung von Leittechniksystemen für Kernreaktoren und zeigt anhand des Beispiels eines modernen digitalen, busorientierten Leitsystems, wie gewisse Systemeigenschaften die nukleare Qualifikation erleichtern können.***

***L'article démontre le principe conservatif qui régit les procédures d'autorisation des systèmes d'instrumentation et de contrôle des réacteurs nucléaires et décrit à l'aide d'un exemple de système de contrôle digital moderne les propriétés particulières qui peuvent faciliter la qualification nucléaire.***

**Adresse des Autors**
*Max Salm*, Zentralstrasse 98, 5430 Wettingen.

## 1. Problemstellung

Die analoge Mess- und Regeltechnik stösst bei komplexen Regelaufgaben an ihre Grenzen; ebenso bei Aufgaben, wo hohe Genauigkeit gefordert ist: sind doch viele Bauteile der elektronischen Analogtechnik durch Temperatur- und Alterungseinflüsse einer sogenannten Drift ausgesetzt. Hier bietet die digitale Technik, d.h. der Einsatz von Mikroprozessoren, enorme Vorteile. Ohne grosse Mehrkosten für die Elektronik können beliebige Verfeinerungen der Regelkreise verwirklicht werden, Parameter können adaptiv durch Prozessgrössen variiert werden, Regelkreise können sogar so ausgelegt werden, dass sie sich selbständig optimieren.

Trotz dieser enormen Vorteile hat sich die neue Technik in fossil gefeuerten Kraftwerken nur zögernd und in Nuklearkraftwerken überhaupt noch nicht durchgesetzt. Dies hat mit den extrem hohen Anforderungen an die Zuverlässigkeit aller Komponenten von Kernkraftwerken zu tun. Obschon bereits heute sehr zuverlässige Datenübertragungsbusse und Mikroprozessoren zur Verfügung stehen, ist es in den meisten Fällen doch äusserst schwierig, ihr Verhalten in Störfällen genau vorauszusagen. Eine solche Analyse ist aber Bedingung zur Erlangung einer behördlichen Genehmigung.

Die zwei hauptsächlichsten Hindernisse, die der Genehmigung von busorientierten Datenübertragungssystemen für nukleare Anwendungen im Wege stehen, lassen sich wie folgt beschreiben:

*1. Datenübertragung:* Die Vorgänge in Kraftwerken sind oft sehr schnell und verlangen deshalb kurze Reaktionszeiten. Die weitaus meisten Datentransportsysteme oder Datenbusse für Kraftwerke werden deshalb im sogenannten Ereignismodus betrieben, d.h. Daten werden nur dann übertragen, wenn sie sich verändert haben. Damit ist aber die Datenübertragungsrate vom Verhalten des Prozesses abhängig. Wenn sehr viele Daten ändern, wird die Übertragung langsamer, ja es gibt sogar Umstände, die zum totalen Ausfall der Datenübertragung führen können. Da das Mikroverhalten der Messgrössen d.h. die Zeitpunkte der minimalen Messwertänderung, die eine neue Datenübertragung auslösen, äusserst schwer vorauszusagen ist, wird es fast unmöglich, die Effizienz der Datenübertragung in allen Fällen nachzuweisen. Es gibt nur wenige, speziell für die Kraftwerksleittechnik konzipierte Datentransportsysteme, die einen rein deterministischen Datenübertragungsmodus aufweisen. Nur eine deterministische Datenübertragung aber hat überhaupt eine Chance, für nukleare Anwendungen qualifiziert zu werden. Auch bei diesen speziellen Systemen bestehen aber im Moment noch Probleme, weil Prüfungsvorschriften für solche Lösungen noch nicht vorliegen.

*2. Mikroprozessoren:* Die meisten auf dem Markt erhältlichen Mikroprozessoren arbeiten mit einem Betriebssystem, das Rechenwerke und Speicher optimal verwaltet. In einem solchen Mikroprozessor kann ein und dieselbe Prozessgrösse zu verschiedenen Zeiten in verschiedenen Rechenwerken verarbeitet und in verschiedenen Speicherzellen abgelegt werden. Auch hier also eine statistische und keine deterministische Arbeitsweise. Es fällt deshalb ausserordentlich schwer, den Nachweis zu erbringen, dass ein Fehler eine ganz bestimmte und eindeutig definierbare Folge hat. Ebenso schwierig wird es sein, nachzuweisen, dass jeder Fehler eindeutig erkannt werden kann. Eine weitere Hürde bildet die Software. Die allgemein verbreiteten Programmiersprachen

enthalten Sprungbefehle, und ein effizientes Programm macht davon reichlich Gebrauch. Schon ein relativ einfaches Programm mit zehn Sprungbefehlen ergibt mehrere Millionen Durchlaufmöglichkeiten. Eine vollständige Analyse des Programms wird damit äusserst aufwendig, ja für komplexe Programme praktisch unmöglich.

## 2. Busorientiertes Leittechniksystem Procontrol P

Wie schon bei der Datenübertragung erwähnt, gibt es auf dem heutigen Markt nur wenige Systeme, die speziell für Kraftwerksanwendungen entwickelt wurden und welche die beschriebenen Probleme grundsätzlich lösen, indem sie deterministisch arbeiten; eine Arbeitsweise, die sonst in der Informatik gänzlich unüblich ist. Als Beispiel dafür seien hier einige Eigenschaften des Leittechniksystems *Procontrol P* der BBC Baden erwähnt.

### 2.1 Datenübertragung

Dieses System wendet bei der Datenübertragung über den Bus grundsätzlich die rein *zyklische Arbeitsweise* an. Diese Methode hat für Kraftwerksanwendungen den Vorteil, dass auf einfache Weise eine sehr rasche Fehlererkennung der Datenübertragung möglich wird, indem jeder Empfänger kontrolliert, ob er zyklisch Daten erhält, und zwar auch dann, wenn keine Änderung der erfassten Prozessgrösse stattgefunden hat. Falls Daten verstümmelt ankommen, wird keine Wiederholung der Übertragung veranlasst, welche die Deterministik stören würde, sondern die letzte korrekte Information beibehalten. Erst wenn in drei aufeinanderfolgenden Zyklen keine korrekten Daten übertragen worden sind, wird ein Fehlersignal generiert. Dieses kann dann eine Fail-Safe-Aktion auslösen.

Die Verwendung der sogenannten *Broadcast-Methode* erhöht die Effizienz der Datenübertragung, indem neben dem Datenwort nur eine Adresse, nämlich die Quellenadresse gesendet werden muss. Auf diese Weise gelingt es in Kraftwerksanwendungen Zykluszeiten von etwa 10 ms zu erreichen; jeder Wert wird damit alle 10 ms aufdatiert und auf seine Richtigkeit geprüft.

### 2.2 Mikroprozessor

Der *deterministischen* Datenübertragung von Procontrol P steht auch ein deterministisch arbeitender Mikroprozessor zur Seite. Alle Datenspeicherplätze sind fix zugeteilt, und die Software enthält keine Sprungbefehle. Jedes Programm wird einmal pro Zyklus (20 ms) Zeile für Zeile abgearbeitet. Die korrekte und rechtzeitige Abarbeitung kann deshalb mit Hilfe relativ einfacher Kontrollschaltungen eindeutig überprüft werden. Selbstverständlich bietet ein solcher Mikroprozessor nicht die gleiche, globale Flexibilität wie die handelsüblichen Geräte. Dies ist auch nicht erforderlich; die schnellen On-line-Regel- und Steueraufgaben lassen sich sehr leicht von den Aufgaben für den Betrieb von Bildschirmen, Druckern usw. trennen. Procontrol P besteht somit aus zwei Teilen:

- der On-line-Regeltechnik mit den speziellen raschen und deterministischen Mikroprozessoren und Datenbussen,
- dem Mensch-Maschine-Kommunikationssystem, das auf handelsüblichen Mikroprozessoren basiert und das rückwirkungsfrei an das Regel-, Steuer- und Datenerfassungssystem angekoppelt ist.

Für die On-line-Regeltechnik sowie auch für alle logischen Funktionen kommt die sogenannte *Funktionsblocksprache* zur Anwendung. Die Funktionsblöcke entsprechen weitgehend den von DIN festgelegten Regel- und Logiksymbolen, so dass die Sprache jedem Regeltechniker von Hause aus verständlich ist. Diese Sprache ist äusserst effizient bei der Verwirklichung aller Steuer- und Regelaufgaben, hingegen enthält sie natürlich überhaupt keine Elemente für die Unterstützung von Rechner-Peripheriegeräten.

### 2.3 Peripheriegeräte

Die Peripheriegeräte sind, wie oben erwähnt, an einem autarken Parallelbus angeschlossen, der nach den üblichen Methoden der Informatik arbeitet. Dieser Kommunikationsbus hat über rückwirkungsfreie Koppelgeräte Zugang zu sämtlichen Daten des Steuer- und Regelteiles. Fehler im nicht deterministischen Kommunikationsteil können sich nicht in den deterministischen Teil hinein fortpflanzen und der Kommunikationsteil hat auch keinerlei Einfluss auf das Zeitverhalten des Steuer-, Regel- und Datenerfassungsteiles.

### 2.4 Qualifizierung für Kraftwerksanwendungen

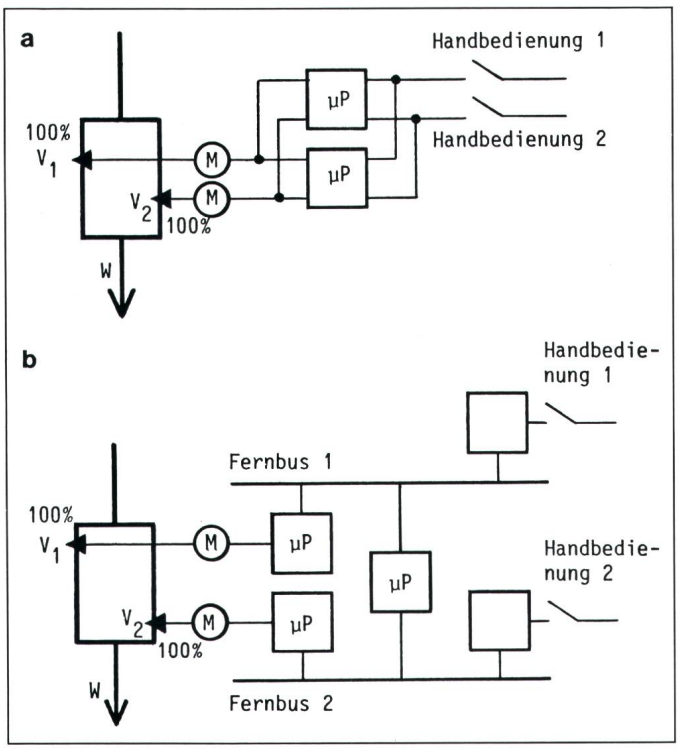
Durch diese klare Trennung dürfte es möglich sein, Procontrol P für Kraftwerksanwendungen zu qualifizieren. Bisher ist dies erst für limitierte Aufgaben geschehen, so z.B. für die Datenübertragung zwischen den Notstandsräumen und dem Hauptkommandoraum im belgischen Kernkraftwerk Tihange oder für die Steuerung und Regelung der Belüftungsanlage des schwedischen Kernkraftwerks Ringhals.

Eine Grundanforderung im Kraftwerk ist die Erfüllung des sogenannten Ein-Fehler-Kriteriums, d.h. ein Einzelfehler, wo immer er auch auftreten möge, darf keinen Ausfall der Produktion und keinen unsicheren Zustand des Kraftwerkes zur Folge haben. Dieser Grundsatz, dem zwar schon immer nachgelebt wurde, geht nach heutigen Sicherheitsbegriffen nicht weit genug. Denn die Frage, was geschieht nachdem ein Einzelfehler aufgetreten ist, bleibt unbeantwortet. Um ganz sicher zu gehen, müsste die Anlage abgestellt werden, denn jetzt könnte jener zweite Fehler auftreten, gegen den die Anlage nicht mehr gesichert ist. Die Wahrscheinlichkeit des Auftretens eines zweiten Fehlers kann beliebig verkleinert werden, wenn die Zeit zur Behebung des ersten Fehlers verkürzt wird. Deshalb wurde Procontrol P mit sehr raschen Fehlererkennungsfähigkeiten ausgestattet und alle elektronischen Geräte wurden so konzipiert, dass sie während des Betriebes ausgewechselt werden können. Da alle permanenten Daten in EPROM gespeichert sind, müssen in einem solchen Reparaturfall auch keine Programme nachgeladen werden. Die ausgewechselten Geräte sind sofort nach dem Einstecken funktionsfähig.

Auch durch geeignete Wahl der Leittechnik-Struktur lässt sich die Zuverlässigkeit eines Prozesses zusätzlich erhöhen, wie das folgende Beispiel zeigt.

### 2.5 Beispiel: Regelung der Speisewasserzufuhr

Das Beispiel enthält einen Regelkreis, der über zwei redundante Stellglieder die Speisewasserzufuhr regelt. Die konventionelle Lösung ist in Figur 1a dargestellt. Die beiden Stellglieder werden von einem gemeinsamen




**Figur 1**
**Beispiel: Speisewasserzufuhrregelung**

M Motorantrieb

$V_1$, $V_2$ Speisewasserventile

W Speisewasser

a Konventionelle Lösung (MTBF = 114 Jahre)

b Dezentrale Lösung (MTBF = 11 322 Jahre)

Mikroprozessor positioniert, wobei der Mikroprozessor sowohl den Algorithmus für die automatische Regelung enthält als auch die erforderliche Logik zum Handbetrieb der Stellglieder. Um dem Einzelfehler-Kriterium zu genügen, ist ein redundanter Mikroprozessor notwendig. Falls dieser eine rasche Fehlererkennungslogik besitzt und ein defektes Gerät ausgetauscht werden kann, während das andere die Aufgabe erfüllt, so resultiert eine rechnerische MTBF (mittlere Zeit zwischen Ausfällen) für die Regelaufgabe von 114 Jahren. Diese Zuverlässigkeitsrechnung enthält die Ausfallraten aller Komponenten, wie Stellglied, zugehörige Schaltanlage, Kabel, Elektronik und Stromversorgung. Dabei ist zu beachten, dass der Betrieb von redundanten Mikroprozessoren keine einfache Sache ist. Viele redundante Mikroprozessorsysteme zeigten im Betrieb Unzulänglichkeiten, und ein bei nuklearer Anwendung unumgänglicher Nachweis der Erfüllung des Einzelfehlerkriteriums ist bei einer solchen Struktur schwierig zu erbringen.

Procontrol P bietet die Möglichkeit, viel dezentralere Leittechnik-Strukturen zu verwirklichen. So zum Beispiel die Variante von Figur 1b. Hier werden die Positionierregelkreise der beiden redundanten Stellglieder auf zwei voneinander unabhängige Mikroprozessoren verteilt, die auch aus zwei verschiedenen Quellen mit Energie versorgt werden. Über zwei voneinander unabhängige Fernbussysteme sind die den Stellgliedern zugeordneten Mikroprozessoren mit einem weiteren Mikroprozessor, der die Algorithmen für automatische Regelung enthält, verbunden. Auch die Befehlsübermittlung von den Bedienungselementen für die manuelle Positionierung erfolgt über die Fernbusse getrennt für Stellglied 1 und 2. Mit dieser Struktur wird der problematische Parallelbetrieb von zwei redundanten Mikroprozessoren vermieden und die Handbedienung der Stellglieder wird zum unabhängigen Back-up für die automatische Regelung.

Führt man gemäss den gleichen Regeln wie für den Fall der Figur 1a eine Zuverlässigkeitsrechnung durch, ergibt sich für den Ausfall der Speisewasserzufuhr eine MTBF von 11 322 Jahren. Trotz mehr Elektronik resultiert allein aus der dezentralen Struktur eine Verbesserung der Zuverlässigkeit um zwei Grössenordnungen.

Beim obigen Vergleich der konventionellen mit der modernen Lösung wurde angenommen, dass bei Ausfall des den Automatikbetrieb steuernden Mikroprozessors, die Speisung des Prozesses durch manuelle Positionierung solange aufrechterhalten werden kann, bis der Mikroprozessor ausgewechselt wird. Das ist bei den Kraftwerksprozessen meistens zulässig und möglich. Hingegen ist nicht in die Rechnung eingegangen, dass in der Struktur 1b kein problematischer Parallelbetrieb von zwei redundanten Rechnern nötig ist. Für die Struktur b wird es deshalb sehr viel einfacher sein, die Erfüllung des Einzelfehlerkriteriums nachzuweisen als bei der Struktur a.

## 3. Ausblick

Die Zukunft wird ohne Zweifel die Bustechnik auch in die Kernkraftwerke bringen. Allerdings werden nur solche Bussysteme eine Chance haben, die deterministisch arbeiten und Strukturen erlauben, die dank Dezentralität zu hohen Zuverlässigkeitswerten führen.