Garant der Sicherheit : die Sicherheit-Leittechnik im Kernkraftwerk

Autor(en): **Bock, Heinz-Wilhelm / Graf, Arnold**

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): **85 (1994)**

Heft 22

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-902623

Der hohe Sicherheitsstandard in der Kerntechnik drückt sich auch innerhalb der Leittechnik aus: Sie umfasst mehrere, gestaffelte Eingriffs-(Interventions-)Ebenen, die entsprechend ihrer sicherheitstechnischen Bedeutung klassifiziert sind und die unabhängig voneinander unzulässige Betriebszustände verhindern. Die Sicherheits-Leittechnik bildet die letzte dieser Interventions-Ebenen, damit kommt ihr bei der sicherheitstechnischen Bewertung die grösste Bedeutung zu.

Garant der Sicherheit

Die Sicherheits-Leittechnik im Kernkraftwerk

■ Heinz-Wilhelm Bock, Arnold Graf

Diese grosse sicherheitstechnische Bedeutung spiegelt sich wider in der besonders hohen Qualität der Sicherheits-Leittechnik; sie drückt sich aus in einer das Übliche weit übersteigenden Fertigungsqualität (TÜV-überwacht und nachprüfbar belegt), in höchster Zuverlässigkeit sowie in strengen, von vornherein festgelegten und vorgegebenen (deterministischen) Auslegungskriterien.

Natürlich kann auch trotz höchster Fertigungsqualität nicht ausgeschlossen werden, dass Komponenten der Sicherheits-Leittechnik ausfallen, da sie wie alle technischen Produkte Alterungseffekten ausgesetzt sind. Deshalb ist die Sicherheits-Leittechnik so aufgebaut, dass auch bei Ausfall von Komponenten die Einleitung sicherheitstechnisch wichtiger Massnahmen nicht verhindert werden kann.

Immer funktionsbereit

Die deterministischen Auslegungskriterien schliesslich schreiben vor, welche Ereignisse bei der Auslegung der Sicherheits-

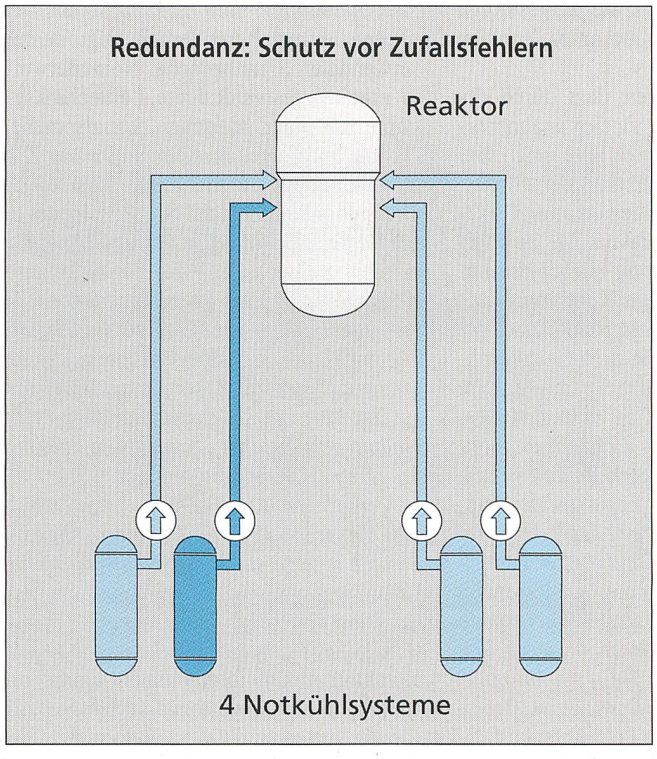

Bild 1 Die einfachste Methode, eine technische Grundsicherheit zu erreichen, ist die zwei- oder mehrfache (redundante) Installation gleicher Systeme oder Geräte, die unabhängig voneinander funktionieren. So sind zum Beispiel für die Notkühlung eines Reaktors vier Kühlstränge installiert, obwohl einer ausreichen würde (Bilder Siemens)

Adresse der Autoren:
Dr. *Heinz-Wilhelm Bock*, Dr. *Arnold Graf*,
Siemens AG, Bereich Energieerzeugung (KWU),
Postfach 32 20, D-91050 Erlangen.

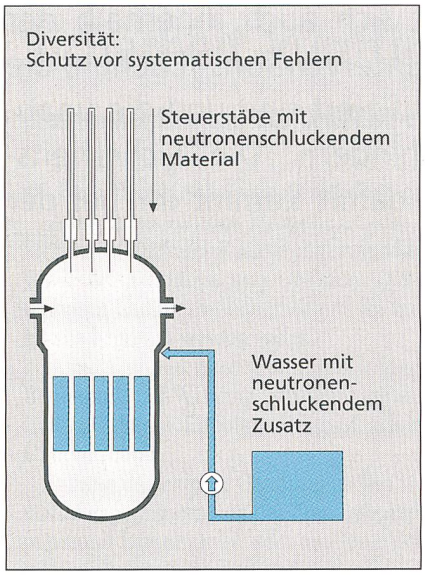

Bild 2 Zwei- oder mehrfach vorhandene (redundante) Systeme könnten aus einer einzigen Ursache heraus gleichzeitig ausfallen, zum Beispiel infolge von gleichen Konstruktionsmängeln oder Fertigungsfehlern. Um sich davor zu schützen, arbeiten die einzelnen Systeme nach verschiedenartigen (diversitären) Prinzipien. Fallen zum Beispiel die Steuerstäbe aus, so tritt sofort die Wassereinspeisung in Aktion, die die Kettenreaktion zum Stillstand bringt

Leittechnik zu berücksichtigen sind. Es sind dies sowohl Naturkatastrophen wie Erdbeben, Stürme oder Überschwemmungen als auch von Menschen verursachte Ereignisse wie Flugzeugabstürze oder Explosionen. Zusätzlich zur nachgewiesenen Qualität und Zuverlässigkeit fordern die deterministischen Auslegungskriterien in Deutschland, dass die Sicherheits-Leittechnik ihre Aufgabe auch bei unterstellten Ausfallkombinationen lückenlos erfüllen muss.

Konkret bedeutet dies, dass durch das gleichzeitige Auftreten zweier unabhängiger Ausfälle einschliesslich aller möglichen Konsequenzen die Funktion der Sicherheits-Leittechnik nicht beeinträchtigt werden darf. Unabhängig davon, wie unwahrscheinlich es ist, muss beispielsweise unterstellt werden, dass ein Kurzschluss auf einer Baugruppe zu einem Brand führt, der alle Einrichtungen im gleichen Gebäudeabschnitt zerstört. Gleichzeitig mit diesem Ausfall ist dann zusätzlich zu unterstellen, dass in einem anderen Gebäudeabschnitt Einrichtungen der Sicherheits-Leittechnik beispielsweise wegen Reparaturmassnahmen nicht funktionstüchtig sind. Entsprechend den deterministischen Auslegungskriterien müssen dann die verbleibenden Einrichtungen in der Lage sein, die Anlage abzuschalten und in einem sicheren Zustand zu halten.

Von besonderer Bedeutung ist dabei, dass auch systematische Fehler als Ausfallursache unterstellt werden müssen. Wird beispielsweise der Füllstand in einem Behälter von mehreren unabhängigen, aber baugleichen Sensoren erfasst, so ist der gleichzeitige Ausfall aller Sensoren anzusetzen.

Mehrfach vorhanden

Struktur und räumliche Anordnung der Sicherheits-Leittechnik sind durch die deterministischen Auslegungskriterien weitgehend vorgegeben. Zur Beherrschung zweier unabhängiger Ausfälle sind in der Struktur mindestens drei voneinander unabhängige (redundante) Stränge vorzuweisen. Da es sowohl aus sicherheitstechnischen wie auch aus wirtschaftlichen Gründen vorteilhaft ist, wenn die Sicherheits-Leittechnik auch während des Betriebs der Anlage geprüft werden kann, haben moderne Druckwasserreaktoren sogar vier voneinander unabhängige Stränge. Die Stränge sind in verschiedenen Gebäudeabschnitten untergebracht und so gegeneinander geschützt, dass bei beliebig angenommenen internen oder auch externen Ereignissen, wie beispielsweise Feuer, Überflutung oder gar Flugzeugabsturz, die sicherheitstechnisch erforderlichen Funktionen ausgeübt werden können. Daher haben diese Stränge selbstverständlich unabhängige Versorgungseinrichtungen wie etwa Lüftungsanlagen oder durch Batterien gepufferte Stromversorgungen.

Dynamische Signale

Eine andere Besonderheit liegt in der verwendeten Signalsprache. Normalerweise arbeiten festverdrahtete Leittechniksysteme mit einer statischen Signalsprache. Das hat zur Folge, dass ein stationärer Zustand im überwachten Prozess auch zu einem stationären Zustand der Signalpegel in der Leittechnik führt. Da nun aber Ausfälle in der Leittechnik, wie beispielsweise Kurzschlüsse oder Unterbrechungen, in fast allen Fällen ebenfalls zu stationären Zuständen der Signalpegel führen, könnte es vorkommen, dass solche Ausfälle die auslegungsgemässe Schutzanregung verhindern und dies bis zur nächsten Prüfung des Systems verborgen bleibt.

Verborgene Ausfälle aber beeinflussen die Zuverlässigkeit gravierend negativ, deshalb ist eine statische Signalsprache für Leittechniksysteme mit höchster Sicherheitsklassifizierung ungeeignet. Daher werden in der Sicherheits-Leittechnik von Kernkraftwerken Leittechniksysteme eingesetzt, die sich einer dynamischen Signalsprache bedienen. Diese zeichnen sich dadurch aus, dass sie ihre Informationen zum Beispiel in Form von Pulsmustern codieren und diese zyklisch übertragen. Das bedeutet beispielsweise konkret, dass die Sicherheits-Leittechnik während des ungestörten Kraftwerkbetriebs – in Pulsmustern codiert – ständig und unmittelbar die Information an die Sicherheitssysteme übermittelt, den Reaktor nicht abzuschalten. Der Wegfall dieser Information wird von den Sicherheitssystemen umgekehrt derart interpretiert, dass der Reaktor spontan abzuschalten ist.

Da nun jeder Ausfall in der Sicherheits-Leittechnik zu stationären Signalpegeln und damit zum Wegfall der Pulsmuster führt, hat er zwangsläufig die Abschaltung des Reaktors und damit einen sicheren Zustand zur Folge. Dieses Verhalten wird üblicherweise als «Fail-Safe-Verhalten» bezeichnet und zeichnet Leittechniksysteme höchster Zuverlässigkeit aus.

Noch mehr Sicherheit durch Prozessortechnik

Für Leittechniksysteme mit dynamischer Signalsprache wurde in der Vergangenheit eine spezielle, auf einzelnen (diskreten) Elementen basierende Gerätetechnik eingesetzt, die sich zur Bildung logischer Signalverknüpfungen auf Magnetkernringe abstützt. Daraus resultiert im Vergleich zu den heute üblichen hochintegrierten Schaltkreisen ein erheblicher Platzbedarf, der bei Nachrüstmassnahmen zunehmend zu Platzproblemen führt.

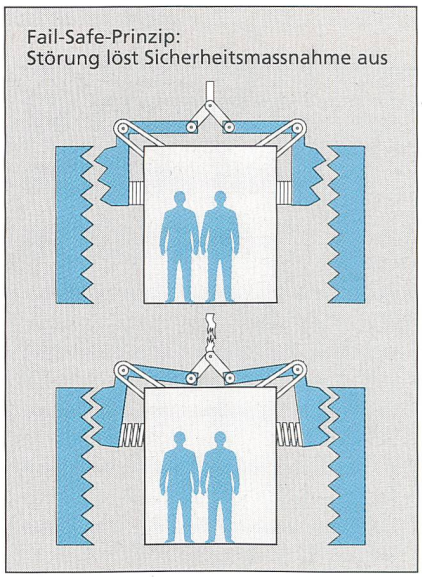

Bild 3 Charakteristisches Merkmal einer Technik, die höchsten Sicherheitsansprüchen genügen muss, ist das «Fail-Safe-Prinzip»: Eine Störung bewirkt durch sich selbst eine Sicherheitsmassnahme. Reisst zum Beispiel bei einem Aufzug das Tragseil, wird durch das Reissen eine Mechanik ausgelöst, die den Aufzug anhält

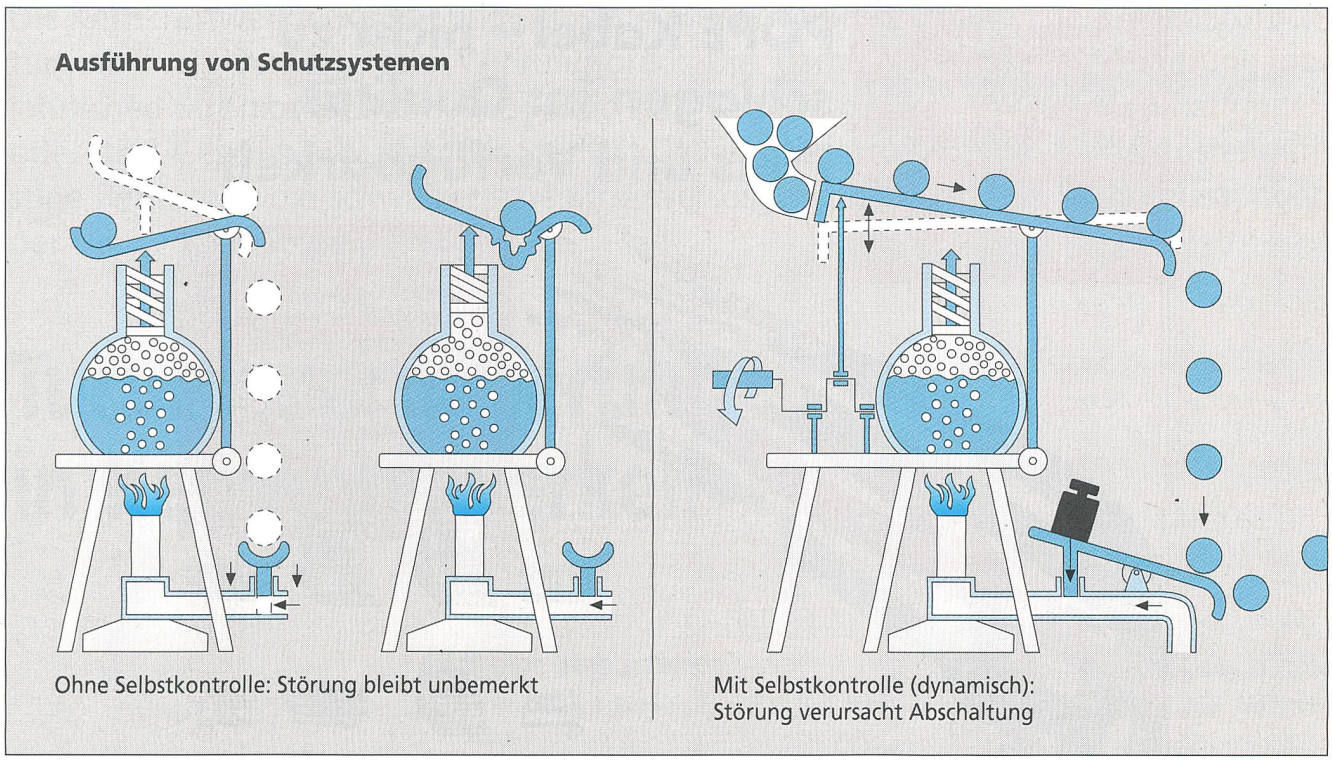

Bild 4 Eine Besonderheit von Leittechniksystemen, die in jedem Fall funktionieren müssen, ist die pausenlose Selbstkontrolle. In Kernkraftwerken ist das durch eine dynamische Signalsprache verwirklicht, die hier in der Modellzeichnung durch pausenlos in bestimmten Abständen rollende bzw. fallende Kugeln symbolisiert ist (anstelle der Kugeln muss man sich elektrische Impulse denken). Sobald die Kugeln ausbleiben oder der Abstand zu gross wird, hat das ständig auf dem Ventil lastende Gewicht keine Gegenkräfte mehr und sperrt die Brennstoffzufuhr automatisch ab

Auf nahezu allen Gebieten der Automatisierungstechnik setzten sich in den vergangenen Jahren programmierbare Prozessor-Systeme durch. Es ist nun von besonderer Bedeutung, dass sich derartige Systeme ebenfalls einer dynamischen Signalsprache bedienen und somit ideale Voraussetzungen für Leittechniksysteme mit «Fail-Safe-Verhalten» bieten.

Prozessoren haben noch weitere Vorteile, die sie gerade für die Realisierung hochzuverlässiger Systeme prädestinieren. Das ist zum einen die Möglichkeit der Selbstüberwachung, durch welche Fehler bereits erkannt werden können, bevor sie zum Ausfall der sicherheitsrelevanten Funktion führen. Zum anderen ist dies die optische Signalübertragung über Glasfaserkabel, welche die Ausbreitung von Ausfällen durch Eintragung von Überspannungen vollständig unterbindet und damit ein ideales Entkopplungsmedium darstellt. Trotz dieser wichtigen positiven Eigenschaften ist die Akzeptanz von Prozessoren in Sicherheitssystemen noch immer nicht unumstritten. Hauptgrund für diese auch unter Experten noch kontrovers geführten Diskussionen ist, dass zur Zeit noch keine Methodik zur Beurteilung der Softwarequalität im Begutachtungsverfahren etabliert ist.

Insbesondere für Anwendungen mit höchster Sicherheitsverantwortung wurde von Siemens in den vergangenen Jahren das auf Prozessoren basierende Leittechniksystem Teleperm XS entwickelt. Ein wesentliches Merkmal dieses Systems besteht darin, dass es eine streng formale Methode zur Softwareerstellung beinhaltet, welches nicht nur höchste Softwarequalität gewährleistet, sondern auch die zugehörige Nachweisführung unterstützt. Daher wird mit Teleperm XS ein wesentlicher Schritt zur Beurteilbarkeit von Softwarequalität erreicht. Die Entwicklung wurde im Auftrag des Bayerischen Staatsministeriums für Landesentwicklung und Umweltfragen (BStLMU) von der Gesellschaft für Reaktorsicherheit (GRS) begleitend begutachtet. In dem im Sommer 1992 fertiggestellten Konzeptgutachten bestätigt die GRS, dass durch das neue, auf Prozessoren basierende System Teleperm XS die Zuverlässigkeit der Sicherheits-Leittechnik in Kernkraftwerken weiter erhöht werden kann.

La technique de commande de sécurité dans la centrale nucléaire

Garant de la sécurité

Le niveau de sécurité élevé de la technologie nucléaire se retrouve également dans la technique de commande. Celle-ci comprend plusieurs niveaux d'intervention échelonnés, qui sont classés suivant leur importance technique et qui empêchent, indépendamment les uns des autres, tout fonctionnement inadmissible. Constituant le dernier niveau d'intervention, la technique de commande occupe ainsi la première place dans l'évaluation technique de la sécurité.

Cette grande importance se reflète dans la qualité particulièrement élevée de la technique de commande de sécurité; elle se traduit par une qualité d'exécution supérieure à la moyenne, une fiabilité exceptionnelle ainsi que des critères de dimensionnement prédéfinis.

Il est clair que la qualité d'exécution optimale n'exclut pas d'éventuelles pannes de composants de la technique de commande, étant donné que ceux-ci sont, comme tous les produits techniques, exposés aux effets du vieillissement. La technique de commande de sécurité est structurée de manière à ce que, même en cas de panne de composants, rien ne vienne entraver le déroulement de mesures techniques de sécurité importantes.