**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:** 85 (1994)

**Heft:** 25

**Artikel:** Wenn's um die Sicherheit geht : spezifische Aspekte eines Gefahrenmeldesystems

**Autor:** Kaufmann, Felix

**DOI:** https://doi.org/10.5169/seals-902644

In der Gefahrenmeldetechnik werden Rechner- und Kommunikationssysteme verwendet, die jenen der klassischen Prozessautomation zwar ähnlich sind, aber doch abweichende Eigenschaften aufweisen. Dieser Artikel beschreibt, welche spezifischen Überlegungen bei der Technik der Gefahrenmeldesysteme gemacht werden und inwiefern diese Technik von derjenigen ähnlich gelagerter Aufgaben abweicht (z. B. Ausfallverhalten). Man wird erkennen, dass nicht zuletzt Kostenüberlegungen zu den heutigen optimierten Lösungen geführt haben. Trotzdem ist nicht zu übersehen, dass der technische und kundenbedingte Druck längerfristig eine Annäherung an standardisierte Systeme erzwingen wird.

# Wenn's um die Sicherheit geht

## Spezifische Aspekte eines Gefahrenmeldesystems

■ Felix Kaufmann

Bei Automatisierungsaufgaben spielt die Steuerungs- und Regelungstechnik eine wichtige Rolle. Die Verarbeitung von Steuer- und Messwerten stellt hohe Anforderungen an die Verarbeitungsalgorithmen, an die Reaktionszeiten und Datenraten. Im Bereich der Gebäudesicherheit eingesetzte Gefahrenmeldesysteme sind auf die Behandlung von Gefahrensituationen zugeschnitten und beschränken sich auf die vergleichsweise anspruchslose Verarbeitung von selten auftretenden Ereignissen. Eine grosse Herausforderung liegt jedoch in der Gestaltung einer Systemarchitektur, welche eine breite Palette von Anforderungen kosteneffektiv abdeckt wie:

- breites Spektrum bezüglich Topologie und Mengengerüst
- unterschiedliche Umgebungsbedingungen ( EMV, Klima…)
- hohe Qualität
- Vorschriftenkonformität
- deterministisches Ausfallverhalten
- hohe Produktelebensdauer und langfristige Produktekontinuität
- Integrationsfähigkeit mit Drittsystemen

Der vorliegende Artikel beleuchtet insbesondere das Ausfallverhalten von Gefahrenmeldesystemen. Dieser Aspekt erlaubt nicht nur eine Differenzierung gegenüber dem konventionellen Leitsystem, sondern auch eine Differenzierung verschiedener Gefahrenmeldesysteme unter sich. Aus dieser Betrachtung lassen sich die Anforderungen an einzelne Systemkomponenten ableiten. Es stellt sich heraus, dass spezielle Mechanismen bei der Konzeption von Netzwerken und Bussystemen wie auch beim Entwurf der elektronischen Baugruppen vorzusehen sind.

### Aufgaben des Gefahrenmeldesystems

Innerhalb eines Gebäudes existieren unterschiedliche Gefahrenquellen. Einige davon sind Brand, Einbruch, das Austreten von Flüssigkeiten oder Gasen. Das Gefahrenmeldesystem beschränkt sich nicht auf das Melden von Gefahren; sein Aufgabenbereich umfasst zunehmend auch die weitergehende Behandlung von Gefahrensituationen. Dazu zählen Aufgaben wie die Gefahrenverifikation, die Löschung, die Evakuierung von Personen, die Unterstützung der Interventionskräfte, die Bereitstellung von Fluchtwegen und die Extraktion von Rauch.

Die Behandlung von Gefahrensituationen erfordert Aktionen des Anlagenbetreibers. Dabei wird er vom Gefahrenmeldesystem massgebend unterstützt. Das

**Adresse des Autors:**
*Felix Kaufmann*, Entwicklungsleiter Systemtechnik, Cerberus AG, 8708 Männedorf.

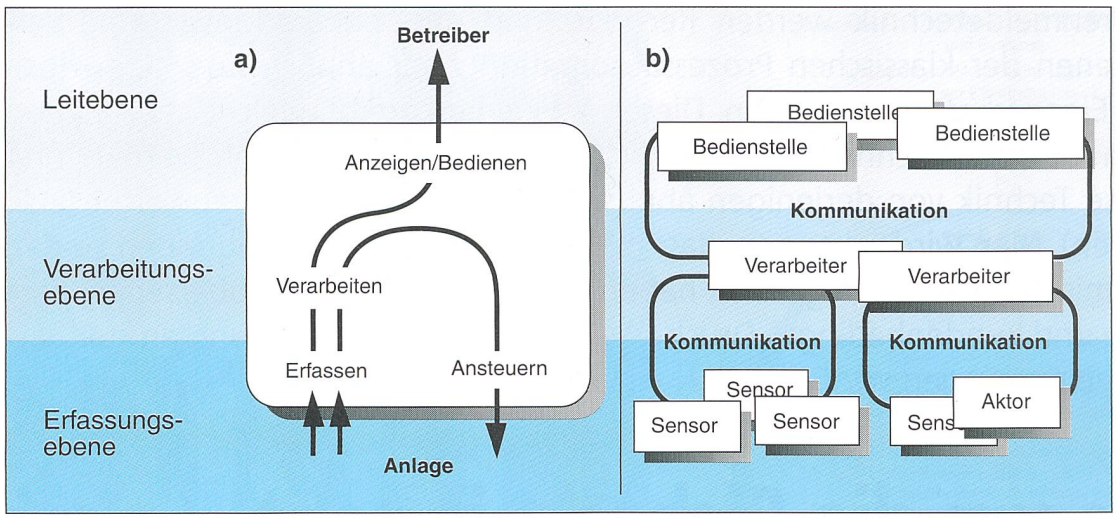


Bild 1a Informationsfluss bei Visualisierung und Steuerung

Bild 1b Architektur eines Gefahrenmeldesystems

Gefahrenmeldesystem bildet das Bindeglied zur Anlage (Bild 1a). Es erfasst die Anlagendaten mittels Sensoren, bereitet diese Daten auf und visualisiert den Anlagenzustand. Zusätzlich wird dem Betreiber der Dialog für die Bedienung des Gefahrenmeldesystems zur Verfügung gestellt.

Der Betreiber hat wenig Möglichkeit, manuell auf die steuerbaren Teile der Anlage einzuwirken. Die Steuerungsaufgaben übernimmt das System selbsttätig. Die Erfassung und Auswertung der Anlagedaten liefert Informationen über Ereignisse, denen zufolge über Aktoren auf die Anlage eingewirkt wird. Die Steuerungsaufgaben sind vielfältig und reichen von der unmittelbaren Gefahrenbekämpfung über die Alarmierung der Interventionskräfte bis zur Ansteuerung von technischen Einrichtungen wie Kameras oder Liftsteuerungen.

Die geographische Ausdehnung von Gebäudeanlagen erfordert immer eine gewisse Dezentralisierung des Gefahrenmeldesystems (Bild 1b). Die geographische Anordnung von Sensoren und Aktoren sowie der Ort für Anzeige und Bedienung ergeben sich aus gebäude- und risikotechnischen Überlegungen.

## Sicherheitsspezifische Vorschriften

Die sicherheitsspezifischen Vorschriften sind länderspezifisch, und der Grad der Reglementierung ist für verschiedene Teilgebiete der Gefahrenmeldetechnik stark verschieden. Sehr weitreichende Bestimmungen existieren für die Brandmeldetechnik. Nebst Funktionen, Antwortzeiten und Umgebungsbedingungen definieren diese Vorschriften massgebend das Ausfallverhalten des Gefahrenmeldesystems. Das Ausfallverhalten ist dann gutmütig, wenn das System trotz Beeinträchtigung zumindest einen wesentlichen Teil seiner Aufgabe weiter erfüllt. Dies bedingt, dass vitale und verzichtbare Leitfunktionen identifiziert werden. Das Erkennen und Melden von Gefahrensituationen gehört beispielsweise zu den vitalen Leitfunktionen. Beim Ausfall der verzichtbaren Leitfunktionen ist der betroffene Anlageteil nur noch degradiert führbar. Beim Ausfall der vitalen Leitfunktionen sind bestimmte Anlageteile nicht mehr führbar. Zur Begrenzung des Risikos definieren die Vorschriften in diesem Falle den maximalen Umfang des betroffenen Anlagenteils.

Der Ausfallsgrad berücksichtigt also zwei Dimensionen: die Funktionsabdeckung und die Anlagenabdeckung. Der Ausfallsgrad lässt sich gemäss Bild 2 schematisieren.

Die Vorschriften definieren ausserdem die potentiellen Fehlerquellen, die zur Beeinträchtigung des Systems führen können. Zunächst wird ein Kurzschluss oder ein Unterbruch von Netzwerken oder Bussystemen in Betracht gezogen, falls das betroffene Kommunikationsmittel ausserhalb eines einzelnen Gerätes geführt wird. Die Vorschriften berücksichtigen als weitere Möglichkeit den Ausfall eines Prozessormoduls sowie den Ausfall der Energieversorgung. In allen Fällen wird von einem Einzelfehler ausgegangen. Mehrfachfehler

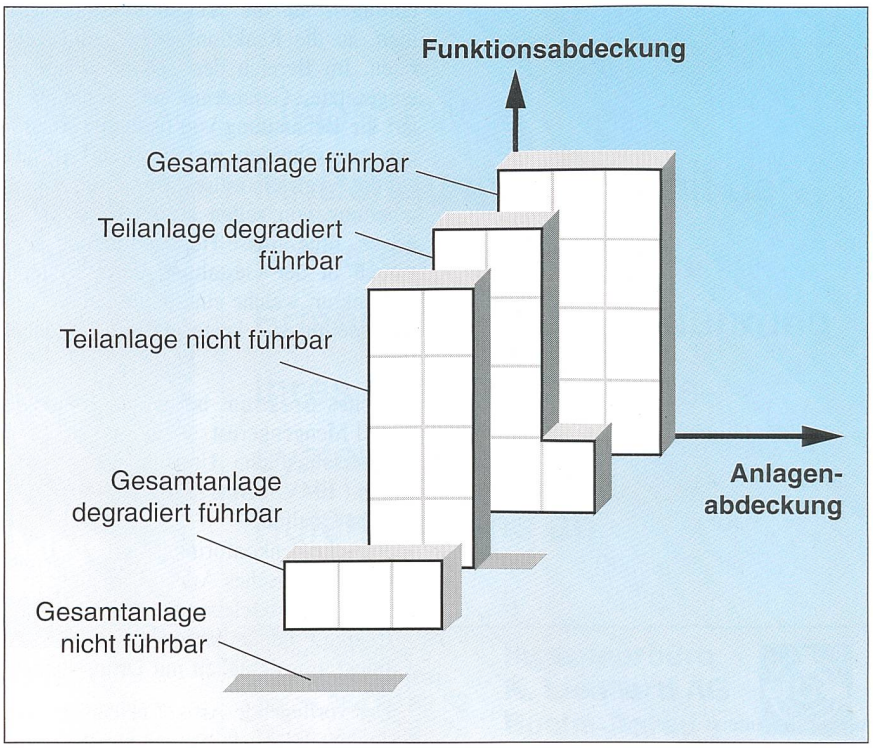


Bild 2 Schematisierter Ausfallsgrad

spielen eine untergeordnete Rolle, da die Erkennung und Anzeige eines Einzelfehlers vorausgesetzt wird.

## Ausfallverhalten nach Mass

Inwieweit erfüllt das Gefahrenmeldesystem die Visualisierungs- und Steuerungsaufgabe auch unter Beeinträchtigung? Diese Frage verlangt eine nähere Betrachtung der Systemarchitektur. Insbesondere kommen sicherheitsspezifische Massnahmen zum Tragen, welche das Ausfallverhalten des Systems gezielt verbessern. Wichtige Massnahmen dieser Art sind die Notstromversorgung und der Notlauf. Der Notlauf ist ein Sicherungsmechanismus, welcher in bestimmten Fehlersituationen die degradierte Führung der Anlage über vitale Leitfunktionen erlaubt. Die Fehlertoleranz bei der Kommunikation führt zu Lösungen, die bezüglich Kurzschluss und Unterbruch unempfindlich sind. Die Dezentralisierung der Systemintelligenz schliesslich beschränkt die Auswirkungen eines Fehlers auf einzelne Anlageteile.

Ausgehend von üblichen Fehlersituationen (gemäss Vorschriften) zeigt die Tabelle I für verschiedene Systemarchitekturen den Ausfallsgrad auf. Der jeweilige Ausfallsgrad wird durch zwei Symbole beschrieben, wobei sich das erste Symbol auf die Visualisierungsaufgabe und das zweite auf die Steuerungsaufgabe bezieht. Die separate Betrachtung ist notwendig, weil sich der Ausfallsgrad je nach Aufgabe und Fehlersituation unterscheiden kann. Die Bedeutung der Symbole selbst ergibt sich sinngemäss aus Bild 2.

Eine konventionelle Architektur antwortet auf viele Fehlersituationen mit einem Totalausfall. Eine sicherheitstechnisch optimierte Architektur zeigt demgegenüber ein gutmütiges Verhalten. Viele Fehlersituationen werden toleriert, andere degradieren die Aufgabenerfüllung mit lokaler Auswirkung, das heisst, nur ein sehr begrenzter Teil der Anlage wird durch den Fehler betroffen.

## Notlauf

Der Notlaufmechanismus ist oft in der Brandmeldetechnik anzutreffen und stellt bei Ausfall eines Prozessors die vitalen Leitfunktionen zur Verfügung. Die Visualisierungsaufgabe beschränkt sich in diesem Fall auf die Sammelanzeige und Quittierungsmöglichkeit von Alarmen. Die örtliche Auflösung zur Lokalisierung der Alarmursache ist markant eingeschränkt. Die Steuerungsaufgabe umfasst im Notlaufbetrieb nur noch die Ansteuerung der Fernübermittlung zur Alarmierung der Interventionskräfte.

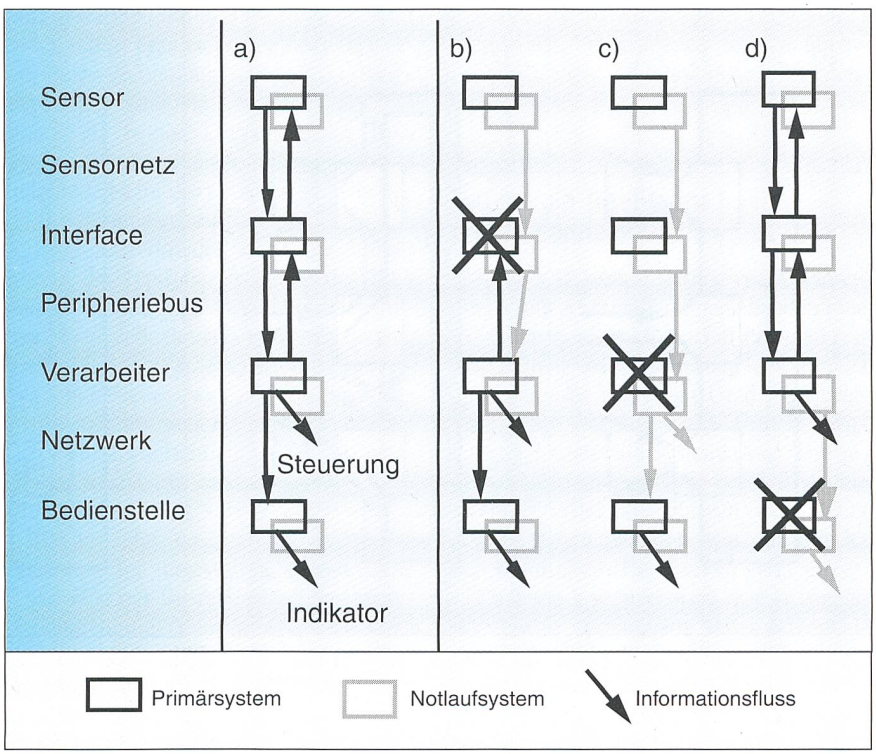


**Bild 3 Das Zusammenwirken von Primär- und Notlaufsystem**
Informationsfluss im regulären Betrieb (a) und Informationsfluss (b, c, d) im Notlaufbetrieb.

Bild 3 zeigt den Informationsfluss, von der Erfassung über die Verarbeitung bis zur Steuerung und Anzeige. Die Information folgt einer Kette von Baugruppen. Das Notlaufsystem verwendet redundante Hardware und gelangt bei Ausfall des Primärsystems selbsttätig zum Einsatz.

Im regulären Betrieb (Bild 3a) ist das Notlaufsystem am Informationsfluss nicht beteiligt. Die Initiative für die Abfrage der Sensoren übernimmt der Verarbeiter. Die Antwort des Sensors gelangt über den regulären Pfad zurück zum Verarbeiter. Dieser löst die notwendigen Steuerfunktionen aus und überträgt die anzuzeigende Information weiter zur Bedienstelle.

| Systemarchitektur / Fehlerart | klassische Architektur | Notstromversorgung + | Notlauf + | fehlertolerante Kommunikation + | dezentrale Intelligenz + |
|---|---|---|---|---|---|
| Prozessorsystem (Leitebene) | — ▯ | — ▯ | ▭ ▯ | ▭ ▯ | ▯ ▯ |
| Kommunikation (Leitebene) | — ▯ | — ▯ | ▭ ▯ | ▯ ▯ | ▯ ▯ |
| Prozessorsystem (Verarbeitungsebene) | — — | — — | ▭ ▭ | ▭ ▭ | ⌐ ⌐ |
| Kommunikation (Erfassungsebene) | — — | — — | ▭ ▭ | ▯ ▯ | ▯ ▯ |
| Prozessorsystem (Erfassungsebene) | ▯ ▯ | ▯ ▯ | ⌐ ⌐ | ⌐ ⌐ | ⌐ ⌐ |
| Energieversorgung | — — | ▯ ▯ | ▯ ▯ | ▯ ▯ | ▯ ▯ |

**Tabelle I Ausfallverhalten verschiedener Systemarchitekturen in Abhängigkeit der Fehlersituation**

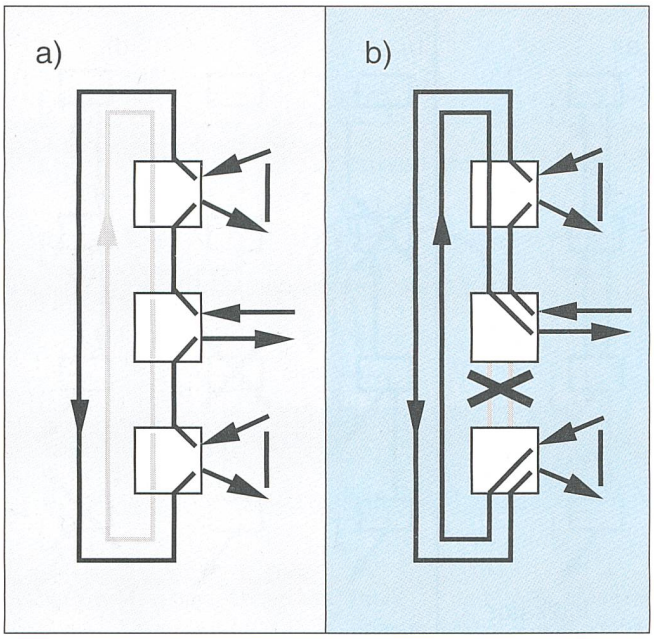


Bild 4 Die Netzwerkankopplung steuert die Informationswege im Ring
a der reguläre Betrieb
b Ausfall einer Verbindung

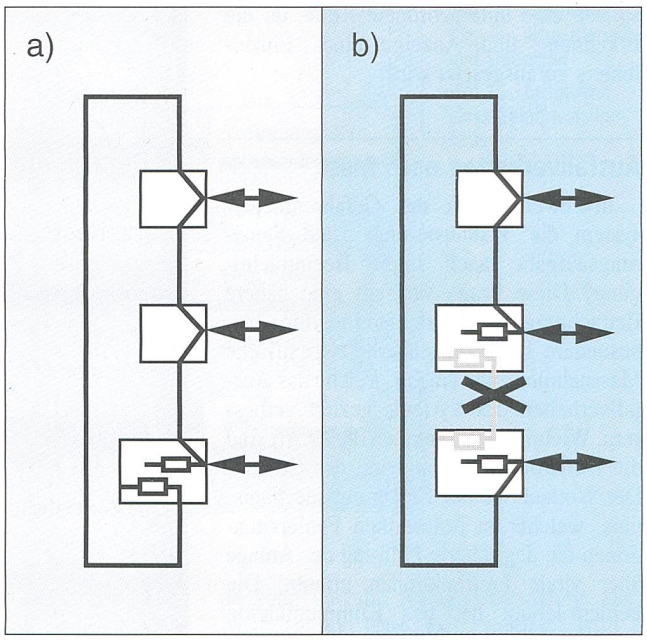


Bild 5 Die Busankopplung terminiert den Bus an den Endpunkten
a der reguläre Betrieb
b Ausfall einer Verbindung

Die reguläre Sensorabfrage setzt die Funktionsfähigkeit von drei Baugruppen voraus, nämlich des Verarbeiters, des Interface und des Sensors. Beim Ausfall einer Baugruppe bleibt die Sensorabfrage aus. Als Konsequenz antwortet der Sensor im Alarmfall (vitale Funktion) über den Notlaufpfad. Wie Bild 3 b, c zeigt, überbrückt der Notlaufpfad die ausgefallene Baugruppe, solange der reguläre Informationspfad nicht benutzbar ist. Die örtliche Auflösung im Notlaufbetrieb ist unterschiedlich. Wenn der Sensor selbst den Notlaufbetrieb verursacht, bezieht sich die Notlaufinformation (Alarm) genau auf diesen Sensor. Wenn das Interface den Notlaufbetrieb verursacht, kann sich die Notlaufinformation auf jeden durch das betreffende Interface bedienten Sensor beziehen. Sinngemäss wird die örtliche Auflösung beim Ausfall des Verarbeiters noch schlechter, zumindest wenn mehrere Interfaces ins Spiel kommen.

Die Baugruppen Verarbeiter und Bedienstelle sind kritische Elemente in bezug auf die Anzeige. Bild 3d stellt den Anzeigepfad bei Ausfall der Bedienstelle dar. Der Indikator zeigt an, wenn ein Alarm ansteht. Eine Einzelterminalkonfiguration gibt jedoch keinen weiteren Aufschluss über den Entstehungsort des Alarms.

Die Informationsmengen sind im Notlaufbetrieb auf einige wenige Bits eingeschränkt, weshalb das Notlaufsystem in der Regel mit einer auf das Problem zugeschnittenen Logik arbeitet. Die Verwendung von redundanten Prozessoren bildet eher die Ausnahme.

Die Kommunikation setzt im Notlaufbetrieb redundante, physikalische Verbindungen zur Informationsübertragung ein. Diese Lösung ist jedoch nicht anwendbar, wenn aus installationstechnischen Überlegungen Zweidrahtleitungen explizit gefordert sind. Die reguläre und die Notlaufkommunikation müssen in diesem Fall die Übertragungsleitungen teilen. Das Übertragungsprotokoll sieht typischerweise zwei Zeitfenster vor. Das eine Fenster dient der regulären, digitalen Kommunikation. Im anderen Zeitfenster gelangen die statischen Pegel zur Auswertung, was für den Notlaufbetrieb genügend Information beinhaltet.

## Fehlertolerante Kommunikation

### Master-Slave-Netzwerke

Für die Kommunikation zwischen Sensor und Verarbeiter (Erfassungsebene) kommen Master-Slave-Lösungen zur Anwendung. Das Interface nimmt die Master-Funktion wahr und bedient die Sensoren bzw. Aktoren als Slave-Teilnehmer. Das Interface spielt beim Auftreten eines Netzwerkfehlers eine wichtige Rolle, indem es die Rekonfiguration des Netzwerkes und damit die Isolation des Fehlers koordiniert.

In der Gefahrenmeldetechnik hat das sogenannte Daisy-Chain-Verfahren nach wie vor eine gewisse Bedeutung. Die Teilnehmer des Kommunikationssystems bilden eine Kette, und jeder Teilnehmer ist mit Trennelementen ausgerüstet. Der Informationsaustausch wird durch das Interface (Master) gesteuert, indem alle Slave-Teilnehmer zunächst vom Netz abgetrennt und schrittweise, entsprechend ihrer Installationsanordnung, wieder zugeschaltet werden. Der Informationsaustausch findet jeweils zwischen dem Interface und dem zuletzt zugeschaltenen Teilnehmer statt. Es ist leicht einzusehen, dass dieser Mechanismus die Erkennung und Isolation eines Netzwerkfehlers (Kurzschluss, Unterbruch) auf einfache Weise zulässt. Der Schritt von der Kette zur Ringstruktur sowie die zweckmässige Handhabung der nunmehr zwei Einspeisestellen in den Ring ermöglichen eine fehlertolerante Lösung zu minimalen Kosten. Dieser Ansatz ist jedoch nur bei ganz bestimmten Netztopologien anwendbar. Eine Ringleitung mit zusätzlich abgesetzten Stichleitungen kann mit geeignet modifiziertem Daisy-Chain-Verfahren noch gehandhabt werden. Die inhärente Kopplung von Netzwerkadresse und Installationsanordnung erweist sich in der Praxis jedoch oft als Nachteil. Ausserdem ist das Verfahren auf bestimmte Störeinflüsse (EMV) empfindlich.

Die obenerwähnten Nachteile treten bei konventionellen Bussystemen nicht auf. Daher verwenden hybride Lösungen die Daisy Chain ausschliesslich für Konfiguration und Rekonfiguration und erfüllen damit die Anforderung nach Fehlertoleranz. Im operationellen Betrieb sind die Netzteilnehmer ständig aufgeschaltet, und der Informationsaustausch erfolgt nach den Regeln eines konventionellen Bussystems.

### Multimaster-Netzwerke

Multimaster-Netzwerke erschliessen die Kommunikation auf der Ebene von Verarbeiter und Bedienstelle (Leitebene). Im Multimaster-Netzwerk existiert kein aus-

gezeichneter Kommunikationsteilnehmer, welcher beim Auftreten eines Netzwerkfehlers die Rekonfiguration des Netzwerks koordinieren könnte. Jeder Teilnehmer nimmt auf der Basis von lokal verfügbarer Information am Rekonfigurationsprozess teil, obschon die Isolation des Fehlers letzlich eine globale Aufgabe darstellt.

Die naheliegende Ringtopologie verbindet die Kommunikationsteilnehmer mittels Punkt-zu-Punkt-Verbindungen. Der Einzelfehler eliminiert genau eine Verbindung, während alle übrigen Verbindungen unbeeinträchtigt zur Verfügung stehen. Der Informationsaustausch zwischen allen Teilnehmern ist nach wie vor möglich; die Informationswege müssen jedoch so geführt werden, dass die ausgefallene Verbindung nicht mehr benutzt wird.

Bild 4 erläutert eine bewährte, in der Sicherheitstechnik eingesetzte Lösung. Bild 4a zeigt die Ringanordnung im ungestörten Zustand. Von der bidirektionalen Verbindung wird nur die eine Richtung (gegen den Uhrzeiger) als Informationsweg genutzt. Die Kommunikation beruht auf der Zirkulation von Meldungen auf dem Ring, wobei der Meldungsstrom von jedem Teilnehmer empfangen und weitergesendet wird. Jede Meldung wird von einem bestimmten Teilnehmer erzeugt und in den Meldungsstrom eingefügt. Die Meldung wird vom gleichen Teilnehmer wieder entfernt, nachdem sie das Netzwerk vollständig passiert hat. Dem Meldungsstrom überlagert, tauschen die benachbarten Teilnehmer Überwachungsmeldungen aus und überprüfen dadurch fortlaufend die Funktionsbereitschaft der Punkt-zu-Punkt-Verbindungen. Der Verlust einer Verbindung durch Kurzschluss oder Unterbruch wird durch genau zwei Teilnehmer festgestellt. Die beiden betroffenen Teilnehmer leiten den Meldungsstrom in umgekehrter Richtung um (Bild 4b). Die übrigen Teilnehmer sind an diesem Rekonfigurationsprozess unbeteiligt.

Die Lösung erlaubt individuelle Übertragungsmedien für die einzelnen Verbindungen. Die Verwendung von Modem-Strecken gestattet auf einfache Weise die Kommunikation über grosse Distanzen. Als Besonderheit dieser Lösung ist zu beachten, dass sich beim Isolieren eines Fehlers die Übertragungszeit verdoppelt. Allerdings sind die Anschlusskosten pro Teilnehmer eher hoch, da nebst der Hardware für die Netzankopplung erhebliche Rechenleistung während des operationellen Betriebs beansprucht wird.

Unter gewissen Einschränkungen ist eine kostengünstigere Lösung möglich. Im Gegensatz zur obenerwähnten Variante besteht das Netzwerk aus einem Bussystem und nicht aus Punkt-zu-Punkt-Verbindungen. Die Installation (Drahtführung) erfolgt zwar als Ring, die Busankopplung sorgt jedoch dafür, dass zu jedem Zeitpunkt genau eine Verbindungsstrecke des Rings aufgetrennt ist. Die Auftrennstelle bestimmt die beiden Endpunkte des Bussystems. Die korrekte Terminierung dieser Endpunkte ist für das zuverlässige Arbeiten des Bussystems erforderlich.

Ein Netzwerkfehler bringt bei dieser Lösung das typische Verhalten des Bussystems an den Tag. Der Unterbruch formiert zwei Teilnehmergruppen, die je eine Insel bilden. Ausserdem wird die Kommunikation unsicher, weil die Terminierung des Bussystems nicht mehr korrekt ist. Der Kurzschluss unterbricht den Kommunikationsaustausch zwischen allen Teilnehmern.

Bild 5a zeigt das korrekt terminierte Bussystem im ungestörten Zustand. Die Zielsetzung der Busrekonfiguration ist offensichtlich: die Trennelemente sind so zu steuern, dass das fehlerhafte Leitungsstück abgetrennt und somit der Fehler isoliert wird. Bild 5b zeigt die Busanordnung nach erfolgter Rekonfiguration.

Das Verfahren zur Rekonfiguration gliedert sich in drei Phasen. Die erste Phase erkennt eine Fehlersituation dadurch, dass beim kontinuierlichen Austausch von Überwachungsmeldungen einzelne Meldungen fehlen. Die Überwachungsinformation erlaubt jedoch keine Rekonstruktion des Fehlerortes. Zur Lokalisierung des Fehlers ist die vollständige Zerlegung des Netzwerks in Teilnetzwerke, die aus genau einem Teilnehmer bestehen, erforderlich. In der zweiten Phase kommt ein statistisches Verfahren zur Anwendung, welches Teilnetzwerke, bestehend aus mehreren Teilnehmern, wieder aufbaut. Der Vorgang wird fortgesetzt, bis wieder genau eine aufgetrennte Verbindung übrigbleibt. Im Gegensatz zur Ausgangskonfiguration ist nun die Verbindung beidseitig aufgetrennt und beinhaltet die Fehlerstelle. Während der Rekonfiguration wird die Kommunikation vorübergehend unterbrochen. Die Anwendungssoftware rekonstruiert in der dritten Phase die während der Rekonfiguration «versäumten» Veränderungen im Gesamtsystem.

Das Konzept ermöglicht Fehlertoleranz mit einem Minimum an zusätzlicher Hardware. Die Trennelemente und der Mechanismus zur Terminierung des Bussystems sind die zusätzlichen Komponenten. Der Algorithmus für die Steuerung der Trennelemente kommt mit der ohnehin vorhandenen Rechnerinfrastruktur aus.

Ein grosser Vorteil des rekonfigurierbaren Bussystems liegt darin, dass fehlertolerante Teilnehmer und konventionelle Busteilnehmer im gleichen Netzwerk gegenseitig verträglich sind. Der Informationsaustausch zwischen allen Teilnehmern ist möglich, Fehlertoleranz ist ausschliesslich zwischen fehlertoleranten Teilnehmern garantiert.

## Dezentrale Intelligenz und Redundanz

Mit der Dezentralisierung von Verarbeitungs- und Anzeigeintelligenz in autonome Einheiten wird beim Ausfall einer einzelnen Einheit die Auswirkung des Fehlers eingeschränkt. Ein hoher Grad an Dezentralisierung verringert die Fehlerauswirkung und erhöht die Systemkosten. Die gegenseitige Unabhängigkeit der Teilsysteme erfordert «Gleichberechtigung» in bezug auf die Kommunikation, was den Einsatz von Multimaster-Netzwerken verlangt.

Einzelne Leitfunktionen, wie beispielsweise eine systemweite Passwortverwaltung, sind ihrer Natur entsprechend zentralistisch und lassen sich nicht ohne weiteres dezentralisieren. Einfache Lösungen sind durchaus möglich, führen aber im Falle eines Fehlers zur Degradation dieser Funktionen. Bei der Passwortverwaltung würde beispielsweise die Eingabe, nicht aber das Verändern der Passworte zugelassen.

Dezentralisierte Lösungen teilen die Intelligenz auf. Redundante Lösungen stellen die gleiche Intelligenz mehrfach zur Verfügung. In der Sicherheitstechnik werden Systeme mit redundanter Verarbeitung vereinzelt angeboten. Dabei handelt es sich um Doppelrechnersysteme mit zusätzlichen Funktionen für die Überwachung der Rechner und für die Umschaltung der gemeinsamen Peripherie.

## Standardnetzwerke auf dem Vormarsch

Das Sicherheitssystem im Verbund mit anderen Systemen der Gebäudeleittechnik ist heute Realität; auf dieser Integrationsebene sind Standardnetzwerke bereits eingeführt. Für die Kommunikation von sicherheitsrelevanten Teilsystemen aber ist die Toleranz von Kurzschluss und Unterbruch eine Forderung, die Standardnetzwerke nach wie vor nicht erfüllen. Für den Bereich der Rechnerkopplung existieren zwar fehlertolerante Kommunikationsmittel, ihre Spezifikationen und Kosten liegen jedoch ausserhalb des für die Gefahrenmeldetechnik in Frage kommenden Rahmens.

Die Forderung nach Multimaster-Fähigkeit wird von einigen Standardnetzwerken erfüllt. Es stellt sich die Frage, ob sich ein Standardnetzwerk mit den sicherheitsrelevanten Mechanismen ergänzen lässt. Bezüglich Notlauf ist dies möglich, falls dem

Notlauf unabhängige physikalische Verbindungen zur Verfügung stehen. Bezüglich Fehlertoleranz sind das Ringnetzwerk und der rekonfigurierbare Bus separat zu betrachten. Beim Ringnetzwerk realisiert das (degenerierte) Standardnetzwerk die Punkt-zu-Punkt-Verbindungen. Das Standardnetzwerk unterstützt verschiedene Übertragungsmedien durch käufliche Produkte. Dadurch entfallen unwirtschaftliche Eigenentwicklungen. Mehr Vorteile bietet der rekonfigurierbare Bus, da er die volle Fähigkeit eines Standardnetzwerkes einsetzen kann und ausserdem die Kommunikation mit standardisierten, käuflichen Netzwerkteilnehmern erschliesst.

Die Hauptanwendung von Feldbussen liegt auf der Erfassungsebene. Die Gefahrenmeldetechnik arbeitet jedoch gerade auf der Erfassungsebene mit spezifischen Lösungen, und beim Entwurf der sicherheitsspezifischen Kommunikation wird die Fehlertoleranz bereits im Konzept berücksichtigt. Auch die additive Ergänzung des Notlaufs scheitert, wenn gleichzeitig Zweidrahtinstallationen gefordert werden. Unter diesen Voraussetzungen hat der Kostendruck bei den Gefahrenmeldesystemen bisher zur Spezialisierung und nicht zur Standardisierung geführt. Deshalb wird zum Beispiel, wenn man anwendungsbezogen optimiert, mit unterschiedlichen Reaktionszeiten für Erst- und Folgeereignis gearbeitet. Die Brandanwendung lässt dies zu; für die Einbruchmeldetechnik ist dieses Verhalten unbrauchbar.

Erste Bestrebungen für die Standardisierung innerhalb der Gefahrenmeldetechnik sind sichtbar. Fehlertoleranz, Reaktionszeit, Installationstechnik, Energieversorgung und Kosten bilden die wichtigsten Eckwerte für den sicherheitsspezifischen Feldbus. Eine Standardisierung schliesst die kompromisslose, anwendungsbezogene Optimierung aus. Die Kosteneinsparung durch Standardisierung sowie die Kosteneinsparung durch elegante Kombination verschiedener Disziplinen der Gefahrenmeldetechnik liegen in der anderen Waagschale. Die nächsten Jahre werden zeigen, ob sich innerhalb der Gefahrenmeldetechnik die Standardisierung auf Erfassungsebene durchsetzen wird.

## Lorsqu'il s'agit de sécurité

### Aspects spécifiques d'un système de signalisation de danger

En technique de signalisation de danger, des systèmes informatiques et de communication sont utilisés, semblables certes à ceux rencontrés en automation des processus industriels classiques, mais possédant des propriétés qui s'en écartent. Cet article décrit les réflexions spécifiques faites en technique de signalisation de danger et dans quelle mesure cette technique se distingue de celle pour des tâches présentant certaines similitudes (p. ex. comportement en cas de défaillance). On se rendra compte que les considérations de coûts n'ont pas été les dernières à conduire aux solutions optimalisées actuelles. Il ne faut cependant pas négliger que la pression technique et conditionnée par la clientèle contraindra à plus long terme à se rapprocher des systèmes standardisés.