



Zweifach sicher vor Ausfall – die Redundanzlösung

Der Aufbau hochverfügbarer Systeme mit echter CPU-Redundanz war bisher meist teuer und dadurch Anwendungen vorbehalten, die bei Ausfällen hohe Folgekosten verursachen. B&R senkt nun die Einstiegshürde zur Hochverfügbarkeit auf ein bisher ungekannt niedriges Niveau. Die Basis bilden Standardsteuerungen der X20-Baureihe, die eine nachträgliche Konfiguration der Ausfallssicherheit in der Softwareumgebung Automation Studio ermöglichen.

Ungeplantes Steuerungsversagen ist nicht tolerierbar. In Zeiten immer knapper werdender Kalkulationen kann der resultierende Produktionsstillstand nicht in den Preis des zu erzeugenden Produktes eingerechnet werden. In Kraftwerken, Chemie- oder Pharmazie-Anlagen, im Offshore-Bereich und auch sonst sind mit einem möglichen Ausfall zudem beträchtliche Gefahren für Mensch und Maschine verbunden. In kritischen Anwendungen, zunehmend häufiger aber auch im klassischen Maschinenbau, wird daher zunehmend der Ruf nach Hochverfügbarkeit durch ausfallssichere, redundante Anordnung aller Steuerungskomponenten laut.

Hochverfügbar durch Redundanz

Redundant ist etwas dann, wenn es mehrfach in gleicher oder sehr ähnlicher Ausführung vorhanden ist. Hochverfügbarkeit wird üblicherweise sichergestellt, indem bei Ausfall einer Systemkomponente eine für diesen Fall bereitgehaltene gleichwertige Komponente die Aufgaben der ausgefallenen übernimmt. Weil die Wahrscheinlichkeit gering ist, dass zwei gleichartige Komponenten gleichzeitig ausfallen, werden hohe Verfügbarkeitswerte erreicht.

Für ein hochverfügbares Gesamtsystem müsste jede einzelne Komponente doppelt ausgeführt und mit einem Umschaltmechanismus für den Versagensfall versehen sein. Allerdings sind dabei die Kosten der Redundanz der Wahrscheinlichkeit und den Folgekos-

ten eines Komponentenausfalls gegenüberzustellen. Daher ist es meist nicht sinnvoll etwa Motoren doppelt auszuführen. Bei Sensoren, Aktoren und I/O-Modulen, meist jedoch Feldbus- oder Netzwerkleitungen, hingegen sieht das anders aus. Das Herz einer redundanten Automatisierung ist die CPU als ihr komplexester Bestandteil, deren Ausfall die folgenschwersten Auswirkungen verursacht.

Redundanzkosten senken

Bisher war der Aufbau ausfalltoleranter Systeme mit redundanten Rechnern oft mit sehr hohen Kosten verbunden und blieb daher auf spezielle Anwendungen – etwa in der Prozessindustrie, in der Energieerzeugung oder in Verkehrssystemen – beschränkt. Der Grund: Dort ist mit sehr hohen Folgekosten oder -schäden zu rechnen.

Mit der CPU-Redundanz für das B&R-X20-System als Teil der Softwareumgebung Automation Studio 4 sinkt diese Schwelle auf einen Wert, der die Hochverfügbarkeit auch für kleine Anwendungen in der klassischen Maschinenautomatisierung attraktiv und wirtschaftlich macht. Zudem ist es den B&R-Entwicklern gelungen, die Funktion so zu gestalten, dass mit Automation Studio 4 erstellte Automatisierungslösungen mit identischen Hardware-Produkten wahlweise mit und ohne CPU-Redundanz ausgeführt werden können. Das eröffnet Maschinenbauern die Möglichkeit, die Aus- »



» CPU-Redundanz darf kein teures Extra sein, das nur Anwendungen mit hohem Schadenspotenzial vorbehalten ist. In den kommenden Versionen von Automation Studio und Automation Runtime ist sie als Konfigurationsmöglichkeit Teil des Standard-Leistungsumfanges. «

Manfred Mitterbuchner, Technical Manager Automation Software bei B&R

» fallsicherheit sehr günstig als Option und sogar auch zur späteren Nachrüstung anzubieten.

Ohne Verzögerung reagieren

In der von B&R gewählten Lösung dient eine Zentraleinheit als prozessführende aktive CPU, die andere läuft nicht-prozessführend im inaktiven Modus. Eine kontinuierliche Überwachung aller Netzwerkfunktionen stellt sicher, dass sie im Ernstfall ohne erneutes Booten die Funktion der aktiven CPU übernehmen kann. Während der inaktiven Phase ist die nicht-prozessführende CPU jedoch keineswegs untätig. Zum einen ist sie durch die Querverkehrsfähigkeit des Feldbusses POWERLINK in der Lage, den gesamten Datenverkehr mitzuhören und damit auch das Synchronisierungssignal der prozessführenden CPU zu überwachen, um ohne Verzögerung innerhalb eines Netzwerkzyklus auf deren Ausfall zu reagieren.

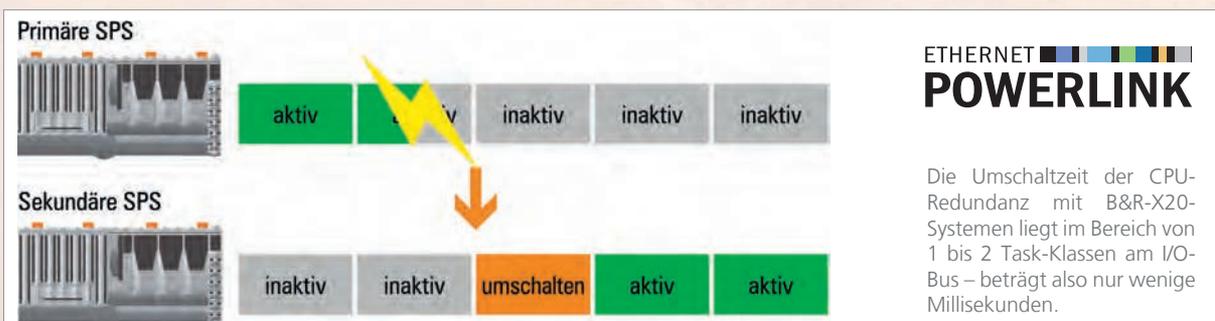
Zum anderen tauscht sie mit dieser über einen Redundanz-Link ständig Daten aus, um taktaktuell auf dem identischen Stand zu sein. Diese vom Feldbus unabhängige, schnelle LWL-Schnittstelle wird durch Redundanz-Interfacemodule hergestellt. Das ermöglicht die Verwendung unveränderter CPUs aus dem X20-Produktportfolio zum Aufbau hochverfügbarer

Systeme. Eigene, wegen der geringeren Stückzahl meist teurere Redundanz-Zentraleinheiten sind somit nicht nötig. Das hält die Initialkosten zusätzlich gering und reduziert auch den logistischen Aufwand.

Darüber hinaus wird es auf einfache Weise möglich, ein System mit geringen Änderungen wahlweise mit oder ohne CPU-Redundanz auszuführen. „Auch aus Sicht eines eventuell übergeordneten Leitsystems ist irrelevant, welche physikalische CPU zur jeweiligen Zeit aktiv ist“, bestätigt Manfred Mitterbuchner, als Technical Manager Automation Software bei B&R verantwortlich für die CPU-Redundanz. „Da die jeweils aktive CPU immer dieselbe IP-Adresse trägt, ist auch an dieser Stelle keine Anpassung erforderlich.“

Umschaltung in wenigen Millisekunden

Eines der heiklen Themen innerhalb der Redundanz ist die Umschaltzeit: Ihre Dauer entscheidet darüber, wie lange eine Anlage quasi im Blindflug läuft oder ob diese Zeitdauer aufgrund der dahinterliegenden Anlagentechnik überhaupt akzeptabel ist. Dieses Thema verliert in der Lösung von B&R weitgehend ihre Brisanz. Der Grund: Die Umschaltzeit der CPU-Redundanz mit B&R-X20-Systemen liegt im Bereich von 1 bis 2 Task-Klassen am I/O-Bus – beträgt also nur wenige Millisekunden.



ETHERNET
POWERLINK

Die Umschaltzeit der CPU-Redundanz mit B&R-X20-Systemen liegt im Bereich von 1 bis 2 Task-Klassen am I/O-Bus – beträgt also nur wenige Millisekunden.

Gegenüber häufig angetroffenen Werten im Bereich von einigen hundert Millisekunden ist das eine maßgebende Größenordnung. Sie ermöglicht eine sehr schnelle und stoßarme Übernahme der Prozessführung im Fehlerfall ohne teure Stillstandzeiten.

Die schnelle Umschaltung zwischen aktiver und inaktiver CPU hat zudem den angenehmen Nebeneffekt, dass die schadhafte Einheit ohne Stillsetzen der Anlage getauscht werden kann, also volle Hot-Plug-Fähigkeit aufweist. Da neu eingesetzte Stationen im Betrieb automatisch synchronisiert werden, kann die Fehlerbehebung von Personal ohne vertiefte Technikenkenntnisse mit sehr geringem Aufwand, vor allem aber auch ohne Beeinträchtigung der Produktivität erfolgen.

Minimaler Engineering-Aufwand

„Um sinnvoll CPU-Redundanz betreiben zu können, müssen in der Systemarchitektur nur wenige Regeln beachtet werden“, sagt Manfred Mitterbuchner. So müssen etwa I/O-Module über die Feldbusse POWERLINK oder Profibus betrieben werden. „Ansonsten ist der Unterschied zu Projekten ohne Redundanz minimal.“

Die Projektierung erfolgt ohne zusätzliches Werkzeug in Automation Studio. Wie bisher projektieren Anwender nur eine Hardware. Projekte mit CPU-Redundanz unterscheiden sich lediglich durch die Deklaration der CPU als redundante Einheit, die auch nachträglich vorgenommen werden kann, sowie durch zusätzliche Eingaben zur Konfiguration von Kommunikationsparametern oder Ausfallkriterien. Alle weiteren Einstellungen werden durch Aufruf der entsprechenden Funktionen von Automation Studio selbständig ergänzt. Abweichend vom Systemvorschlag können Prozessvariablen und Bibliotheken auch einzeln als redundant oder nicht-redundant definiert werden. Die Systemphilosophie von B&R kommt zum Aufbau hochverfügbarer Systeme mit echter CPU-Redundanz ohne spezielle CPUs aus. Unabhängig voneinander erfolgen sowohl die Programmierung der Applikation als auch die optionale Konfiguration der Ausfallssicherheit in der einheitlichen Softwareumgebung Automation Studio. So senkt B&R die Einstiegshürde zur Hochverfügbarkeit auf ein Niveau, das sie auch für den Serienmaschinenbau interessant macht. ■

