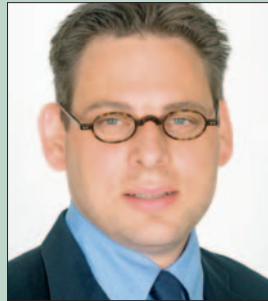


STANDPUNKT SIND INTEGRIERTE SICHERHEITSSYSTEME SICHER GENUG?

Bietet ein integriertes Sicherheitssystem genug Sicherheit? Yokogawa integriert sicherheitsgerichtete Steuerungen ins PLS, Tim Henrichs erklärt warum. Rolf Hafner, als Vertreter der Safety-System Experten von Hima, spricht dagegen.

PRO



Die Integration der sicherheitsgerichteten Steuerung in das Produktionsleitsystem bietet einige Vorteile, die bei nicht integrierten Systemen nicht möglich sind. Dazu gehören eine Betriebsumgebung mit einheitlicher Bedieneroberfläche, Trending, Alarmmanagement, Sequent of Event, Status Anzeige und das integrierte Feldgerätemanagement. Auch für die Zeitsynchronisierung muss kein zusätzliches Netzwerk aufgebaut werden. Die IEC 61508-2 fordert die Trennung der Sicherheitsgerichteten von der Prozesssteuerungsfunktion, somit steht dies erst einmal im Widerspruch zum eigentlichen Anspruch einer integrierten sicherheitsgerichteten Steuerung.

Wie trennt ein Hersteller die beiden Aufgaben in einem integrierten System? Die Lösungen sind herstellerspezifisch und müssen an den Anforderungen gespiegelt werden. Ganz nach dem Motto „integriert aber separat“ sollte die Integration rückwirkungsfrei auf den Informationsaustausch (Informationstransparenz) begrenzt sein. Zusätzlich ist darauf zu achten, dass sich die beiden Systeme in keiner Weise bei den upgrade Regularien beeinflussen.

Nicht nur technisch werden die Schnittstellen zwischen dem sicherheitsgerichteten Bereich und dem Prozessbereich minimiert, sondern auch in der Projektabwicklung und Pflege der Systeme. So müssen weder Schnittstellenlisten zwischen Herstellern abgeglichen, noch Zeit für Integrationstests aufgewendet werden. Auch für die Inbetriebnahme und für den Lebenszyklus der kompletten Automatisierung gibt es nur einen verantwortlichen Hersteller.

Tim Henrichs, Produktmanager Systeme bei Yokogawa

CONTRA



Die IEC 61511 fordert den Erhalt sämtlicher Independent Protection Layers (IPL). Für jede dieser Schutzschichten wird Unabhängigkeit, Diversität und physikalische Trennung verlangt. Nur wenn Sicherheitssystem und Prozessleitsystem auf ungleichen Plattformen, Entwicklungsgrundlagen und Philosophien basieren, sind sie autark und damit in der Lage, sich als separate Schutzschichten gegenseitig „Kredit“ zu geben, damit Common-Cause- und systematische Fehler verhindert werden. Selbst zahlreiche Änderungen oder Updates im Prozessleitsystem bleiben so rückwirkungsfrei und können die Performance des Sicherheitssystems wie beispielsweise Zykluszeiten nicht beeinträchtigen.

Über 85 Prozent aller Fehler die zu Unfällen geführt haben, sind menschliche Fehler. Deshalb sollten im Safety-Management nur Spezialisten arbeiten, die viel Erfahrung mit Sicherheitstechnik, speziell bei der Technik-Auswahl mitbringen und sich bei Wartungs- bzw. Änderungsmaßnahmen genauso gut auskennen wie bei Normen und rechtlichen Vorschriften. Im Übrigen müssen die personellen Zuständigkeiten klar organisiert sein. Alles dies und die klare Trennung der Systeme ist notwendige Voraussetzung dafür, um als verantwortlicher Anlagenbetreiber den Status der „Best Engineering Practices“ und damit Rechtssicherheit zu erlangen.

Fakt ist: Die Trennung zweier autarker Systeme ermöglicht trotzdem deren Integration. Mit Hilfe innovativer Technik und dank offener Standards kann Hima das heute komfortabel mit jedem führenden Prozessleitsystem verwirklichen.

Rolf Hafner, Leiter Produktmanagement bei Hima

[> MORE@CLICK PA310202](#)