Den Faktor Mensch ausbremsen

Funktionale Sicherheit bei Temperatur-Transmittern

Jens Baar

Sicherheit wertschätzen nahezu alle Menschen als hohes Gut. Deswegen sollten alle Möglichkeiten dazu ausgeschöpft werden. Dass es keineswegs so ist, zeigt der Sicherheitsgurt im Auto. Das Anlegen müsste ein automatischer Handgriff sein. Dennoch verfügen alle Neuwagen über eine akustische Anschnall-Überwachung – weil der Mensch am Steuer schon mal das Angurten vergisst. In Fragen der Sicherheit gibt es in der Prozessindustrie ähnlich gelagerte Entwicklungen, zum Beispiel beim Einsatz von Temperatur-Transmittern.

Autor: *Jens Baar, Produktmanager elektrische Temperaturmesstechnik, WIKA, Klingenberg*

Wie bei den Schutzmechanismen im Straßenverkehr sind in der Prozessindustrie die Ansprüche an die „funktionale Sicherheit", so der Terminus, in den vergangenen Jahren gestiegen. Diverse Sicherheitssysteme minimieren das Risiko, das von einer Anlage ausgeht. Für das höchstmögliche Maß an Sicherheit stehen drei Buchstaben: SIL. Nach den Maßgaben dieses Safety Integrity Level werden immer mehr Applikationen zertifiziert, in Werkskonglomeraten wie bei großen Chemieunternehmen sind es bis zu 20 %. Die Klassifizierung von SIL 1 bis 4 richtet sich nach dem jeweiligen Gefährdungsgrad.

Sollen Sicherheitssysteme von Industrieanlagen nach SIL zertifiziert werden, dürfen sie ausschließlich Geräte enthalten, die nach DIN EN 61508 bzw. EN 61511 (speziell für die Prozessindustrie) entwickelt oder qualifiziert sind. Beiden Normen spezifizieren die Anforderungen an das Verhalten des Instrumentariums. Allerdings gibt es hierbei durchaus einen gewissen Interpretationsspielraum.

Anforderung an die Geräte

Ein wesentliches Element solcher Sicherheitssysteme sind intelligente Endgeräte wie Temperatur-Transmitter. Sie verfügen über eine Software, mit der sicherheitsrelevante Parameter wie Messbereich, Sensoreinstellung und Fehlersignalisierung

nach Prozessbedarf flexibel geändert werden können. Das Schützen dieser Programme wird ebenfalls in den SIL-Vorschriften behandelt. Im Teil 3 der Norm EN 1508 heißt es: „Betriebsparameter müssen geschützt werden gegen: ungültige Werte (…) zur falschen Zeit/unbefugte Änderungen/Verfälschung“. Der entsprechende Auszug der EN 61511 aus Teil 1 lautet: „Änderbare Parameter sollten auf Schutz vor Folgendem geprüft werden: (…)/falsche Werte/unberechtigte Veränderungen(…).“

Beide Formulierungen lassen den Schluss zu, dass die Entscheidung, ob eine Geräte-Software tatsächlich „verriegelt“ wird, letztlich in die Kompetenz des Anwenders fällt. Deswegen bieten auch viele Temperatur-Transmitter lediglich die Möglichkeit, das Programm vor ungewolltem Zugriff zu schützen. Bei solchen Einstellungsänderungen hat man weniger gezielte Manipulationen vor Augen als den Risikofaktor Mensch. Wie schnell kann im Zweifelsfall jemand zum Beispiel den Messbereich abwandeln, weil er trotz Warnsignal den Anlagenbetrieb nicht unterbrechen möchte. Welche Folgen ein solches Handeln haben kann, muss hier nicht vertieft werden: Ausfall der Anlage, Tonnen von Produktionsausschuss, Verletzungen. Alles wesentlich gravierender als die Konsequenzen, die sich aus dem Detektieren der gemeldeten Störung ergeben.

Da aber die maßgeblichen Normen nun einmal fordern, das Gerät vor unbefugtem Zugriff auf die Konfiguration zu schützen, kann das Risiko nur auf einem Weg eingedämmt werden: Die Messgeräte müssen von vornherein über eine elektronische Verriegelung verfügen, also über eine Schreibschutz-Funktionalität. Auch hierbei bietet die Kfz-Technik einen Vergleich. Bei vielen Autos kann der Motor nur bei gedrücktem Kupplungspedal gestartet werden, ein ungewolltes Vorwärtsspringen des Autos durch den eingelegten ersten Gang wird so ausgeschlossen – und damit die Gefahr eines Unfalls.

Bei einem Transmitter mit Zugriffssperre wird dem Anwender kein Spielraum gelassen: Sein Gerät lässt sich nur dann konfigurieren, wenn zuvor der Schreibschutz mittels eines Passworts deaktiviert wurde. Nach der Programmierung wird die Schutzfunktion wieder aktiviert, ein ungewollter Zugriff bei laufendem Betrieb ist nicht mehr möglich.

Schreibschutz für SIL-Geräte

Dieses Plädoyer für Transmitter und verwandte Produkte mit Konfigurationsschutz bedeutet kein Aufruf, die Gerätelandschaft in Industrieunternehmen komplett umzukrempeln und ältere Mess- und Regeltechnik, die unter dem Signum „Betriebsbewährtheit für Sicherheitsanwendungen“ läuft, umgehend auszutauschen. Ein solches Unterfangen wäre schlechthin undurchführbar. Aber bei aktuellen SIL-Geräten sollte implementierter Schreibschutz zwingend sein. Damit wäre gewährleistet, dass nur ein autorisierter Personenkreis den Kontrollmechanismus den jeweiligen Anforderungen anpassen bzw. in kritischen Phasen die erforderlichen Schritte einleiten kann.

Der notwendige Mehraufwand wird durch das Ausschalten des „menschlichen“ Restrisikos mehr als wettgemacht: Er verhindert deutlich Schlimmeres, mag die Wahrscheinlichkeit eine solchen Schadensfalles noch so gering sein. Um beim Straßenverkehr zu bleiben: Schon bei einem Aufprall mit geringem Tempo bricht man unangeschnallt mit dem Gesicht durch die Windschutzscheibe. Dabei wollte man doch bloß mal eben um die Ecke fahren.

Digitaler Temperatur-Transmitter mit Hart-Protokoll, Kopfversion

Wika www.vfmz.net/**1034140**