



Safety inklusive

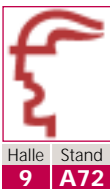
Im Zuge einer Anlagenmodernisierung wurde im Kernkraftwerk Biblis erstmals ein Rundlaufkran mit einer Steuerungslösung nachgerüstet, bei der Standard- und sicherheitsgerichtete Programme auf demselben Controller ablaufen und über einen Standard-Feldbus mit der fehlersicheren E/A-Baugruppe kommunizieren.

Die sicherheitstechnische Ausführung von Hebezeugen hat in Kernkraftwerken einen besonderen Stellenwert. Wo auf das Vierfache der Nennlast ausgelegte mechanische Festigkeiten üblich sind, stellen die Zulassungsbehörden auch an die Automatisierungstechnik höchste Anforderungen. Definiert sind diese in den sicherheitstechnischen Vorschriften des Kerntechnischen Ausschusses KTA 3902, Kategorie 4.3. Ein Regelwerk, welches zur Standardlektüre der rund 30 Mitarbeiter der Lorasch GmbH gehört.

Das Unternehmen mit Sitz im fränkischen Gemünden ist spezialisiert auf die automatisierungstechnische Modernisierung und Wartung von Großkran-Anlagen und erhielt 2003 den Auftrag, einen Reaktor-Rundlaufkran im Kernkraftwerk Biblis mit fehlersicherer SPS-Technik nachzurüsten.

Die Kran-Konstruktion hat eine Spannweite von rund 40 Metern und verfügt über drei Hubwerke für Nennlasten von 200 (Haupthub), 40 (Hilfshub) und 5 Tonnen (Sonderhub). Sie ist in 39 Metern Höhe unter der Kuppel installiert und wird

für sämtliche Lastbewegungen im Regelbetrieb und vor allem während der Revisionen eingesetzt. Beispielsweise zum Transport des Reaktordeckels, von Deckelspannvorrichtungen, Trennschützen, Traversensätzen und anderen Schwerlasten. Ein Ausfall der Anlage würde gerade bei einer Revision, wenn über Wochen hinweg bis zu 1500 Mann rund um die Uhr im Kraftwerk arbeiten, nicht nur erhebliche finanzielle sondern insbesondere auch sicherheitsgefährdende Auswirkungen haben.



Halle Stand
9 A72

(Grafik: Computer & AUTOMATION, Quelle: Siemens)



Die hohen Sicherheitsanforderungen der KTA 3902, Kat. 4.3 schreiben aus diesem Grund vor, dass bewegte Lasten und die Abschaltungen der Hubwerke in den Endlagen laufend überwacht werden müssen, um Schäden an Personen und Einrichtungen sicher zu vermeiden. Früher wurde dies mit extrem aufwendigen Relais- beziehungsweise Schützsteuerungen realisiert, in jüngerer Zeit mit doppelt ausgeführten SPS-Steuerungen. Im jüngsten Projekt ist Lorasch jetzt noch einen Schritt weiter gegangen und hat erstmals eine Lösung realisiert, die mit nur noch einer CPU, einer fehlersicheren Simatic S7-300 mit CPU 315F-2 DP, und darauf abgestimmten fehlersicheren Ein-/Ausgabebaugruppen für das dezentrale Peripheriesystem ET 200M von Siemens auskommt.

Die insgesamt sechs 4- bis 20-mA-Signale aller drei Lastmessbolzen werden im sicheren Betrieb über fehlersichere Analog-Eingabebaugruppen vom Typ SM 336 redundant erfasst, mit einer Auflösung von 13 Bit digitalisiert und über Profibus-DP zur fehlersicheren Steuerung übertragen. Diese überprüft für jeden Bolzen laufend die Abweichung der beiden Signale voneinander und schaltet

beim Überschreiten der zulässigen Toleranz sofort in einen sicheren Zustand. Abschalt- und andere Steuersignale gelangen ebenfalls über fehlersichere digitale E/A-Baugruppen von und zu den Aktoren und Sensoren, darunter über Profibus angebundene Antriebe.

Interne und externe Fehlerdiagnose

In Summe sieht das Steuerungskonzept eine zentrale und sechs dezentrale E/A-Baugruppen vor, wovon ein Teil Standard- und sicherheitsgerichtete Signale nebeneinander überträgt. Konkret handelt es sich dabei um 136 digitale Standard-Eingänge, 64 digitale Standard-Ausgänge, 24 digitale fehlersichere Eingänge, 30 digitale fehlersichere Ausgänge und 6 analoge fehlersichere Eingänge. Die fehlersicheren Peripheriebaugruppen – optisch erkennbar am gelben Beschriftungsstreifen – sind intern redundant aufgebaut und können interne wie externe Fehler diagnostizieren. Mit integrierten Selbsttests erfüllen sie wie die F-Controller die Sicherheitsanforderungen nach IEC/EN 61508 (bis SIL 3), EN 954 (bis Kat. 4), NFPA 79 – 2002 und NFPA 85.



Der Aufbau der Automatisierung konnte zu fast 99 % bei Lorasch im Haus erfolgen. Über einfache Schalter wurden dort die 128 theoretisch möglichen Störursachen simuliert. Dies reduziert die Inbetriebnahmezeit vor Ort im Kernkraftwerk, wo neben verschärften Strahlenschutzbedingungen auch immer chronischer Zeit- und Platzmangel herrschen, auf ein Minimum.

Weitere Aufgaben dieses Verbunds sind die Überwachung der oberen und unteren Endlagen der drei Hubwerke sowie die Kontrolle der galvanischen Trennung beim Umschalten von der Funkfernbedienung auf das konventionelle Steuerpult. Zur Anzeige der jeweiligen Traglast (in Tonnen) dienen zwei große Leuchtanzeigen, die als DP-Norm-Slaves von der SPS angesteuert werden.

Separater Sicherheitsbus entfällt

Dadurch, dass bei der skizzierten Steuerungslösung sowohl das Standard- als auch das sicherheitsgerichtete Programm in einer Steuerung ablaufen, und die fehlersichere Kommunikation mit Hilfe des Profisafe-Protokolles über „Standard“-Profibus-DP-Leitungen geführt werden kann, erspart sich Lorasch den bisher für diese Anwendung erforderlichen zweiten Controller und auch den separaten Sicherheitsbus, ohne den klassische Sicherheitssteuerungen nicht auskommen. „Der Hardware- und Verdrahtungsaufwand“, so Dieter Häußler, Leiter der Elektrotechnik bei Lorasch, „reduziert sich dadurch für uns auf etwa die Hälfte!“

Als Plus der SPS-Technik allgemein wertet Häußler die hohe Flexibilität, etwa bei der Optimierung oder bei nachträglichen Änderungen. Während konventionelle, fest verdrahtete Sicherheitsinstallationen nur mit immensem Aufwand verändert werden können, lassen sich fehlersichere SPS-Programme bis zum Schluss einfach und komfortabel editieren. Änderungen am Standard-Programm sind auch noch nach der Abnahme des sicherheitsrelevanten Teils möglich.

Engineering wie gewohnt

Neben dem Basis-Engineering-Paket von Siemens nutzte Lorasch zusätzlich das Optionspaket „S7 Distributed Safety“. Außer einer Bibliothek von TÜV-zertifizierten Baustein- und Applikationsvorlagen für sicherheitsgerichtete Aufgaben, steht dem Anwender hier ein Befehlsvorrat auf Basis von F-KOP und F-FUP, den sicherheitsrelevanten Äquivalenten der Standardsprachen KOP (Kontaktplan) und FUP (Funktionsplan), zur Verfügung, auf dessen Grundlage sich Lorasch eigene Failsafe-Bausteine generiert hat.

Die Safety-Lösung fügt sich somit nahtlos in die Simatic-S7-Umgebung ein; zudem besteht eine Durchgängigkeit der Automatisierungslösung über F-Steuerung, F-Peripherie, Antriebe und HMI-Technik hinweg. Auf Grund der gemeinsamen Datenhaltung, der vereinheitlichten Kommunikation sowie über das integrierte Projektieren und Programmieren lassen sich der Engineering-Aufwand um mindestens 30 % verkürzen im Vergleich zu einer konventionellen Realisierung mit Sicherheitsrelais – so die Erfahrungen im Hause Lorasch mit dem neuen Safety-Konzept.

(Bild: Siemens)