Funktional sichere Elektronik kosteneffizient entwickeln

Safety-Anwendungen für die Fabrikautomation schneller entwickeln

Der Factory Automation Markt fordert zunehmend Safety-Lösungen, die sowohl den Anforderungen gemäß IEC 61508 als auch den Anforderungen der ISO 13849-1 entsprechen. Sollen hierbei Performance Level (PL) d oder e erreicht werden, ist zu beachten, dass die Anforderungen an die Sicherheitsarchitektur gemäß Kategorie 3 oder 4 teilweise höher ausfallen. Vorzertifizierte Safety-System-on-Chip (SoC) Lösungen helfen, unnötige Risiken und Mehrkosten im Entwicklungsprozess zu vermeiden sowie die Time-to-Market deutlich zu verkürzen.

IEC 61508 ist nicht gleich ISO 13849-1

Bei Hard- und Softwareentwicklern im Bereich der Fabrikautomation ist der Trend festzustellen, immer mehr Steuerungslösungen sowohl gemäß den Anforderungen der allgemeinen Norm für Funktionale Sicherheit von elektronischen Systemen IEC 61508 als auch gemäß der ISO 13849-1 für die Sicherheit von Maschinensteuerungen auszulegen. Vielen Automatisierern, welche nicht jeden Tag mit Safety zu tun haben, ist nicht bewusst, dass die Sicherheitsanforderungen der ISO 13849-1 in PL d oder PL e der Kategorie 3 oder 4 hinsichtlich Architektur höher ausfallen können als bei der IEC 61508. So fordert erstere zwingend ab Kategorie 3 eine Zweikanaligkeit aller sicherheitsrelevanten Strukturen, was für SIL-Applikationen nicht zwingend notwendig ist. Dies kann dazu führen, dass es bei der TÜV-Zertifizierung zum bösen Erwachen kommt, wenn sich herausstellt, dass das entwickelte Konzept die ISO 13849-1 gar nicht oder nur unter hohem Extraaufwand erfüllen kann.

Automatisierungstechnikhersteller entscheiden sich bislang in der Praxis meist für eine der folgenden Optionen, um die geschilderte Problematik zu lösen:

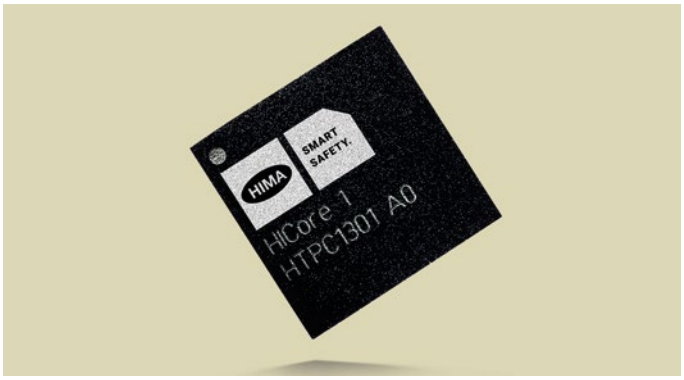
A) Sie wählen eine SoC-Plattform, die den Anforderungen der ISO 13849-1 genügt, aber nicht entsprechend zertifiziert ist. Hier erfüllt die entwickelte Lösung zwar theoretisch die technischen Anforderungen, die aufwendige Zertifizierung muss jedoch in Eigenregie durchgeführt werden. Dies treibt die Entwicklungskosten in die Höhe und verlängert signifikant die „Time-to-Market".

B) Sie setzen eine Lösung auf Basis von Standardkomponenten mit zwei getrennten Prozessoren und diskreter Sicherheitslogik um. Bei dieser häufig gewählten Variante fallen die Entwicklungskosten noch höher aus als bei Option A, da Anwenderprogramm und Logik jeweils zweimal fast analog entwickelt werden müssen. Darüber hinaus birgt sie unwägbare Risiken, bis hin zum kompletten Scheitern des Projekts, wenn erst im Laufe der Entwicklung festgestellt wird, dass die konzipierte Lösung die Kriterien der ISO 13849-1 bis PL e und Kat. 4 nicht, oder nur kostenintensiv erfüllen kann. Darüber hinaus kann Obsoleszenz zum Problem werden, da die Lebenszyklen von Produkten in der Factory Automation deutlich länger sind als bei Standardelektronikkomponenten.

C) Sie zielen in der Entwicklung, wenn möglich, auf die Realisierung niedrigerer Sicherheitsanforderungen (z.B. SIL 2 / PL c). In diesem Fall verfehlen sie das ursprünglich gesteckte Entwicklungsziel und erreichen nicht den im Projekt geforderten Sicherheitsstandard.

Auf der sicheren Seite mit dem zertifizierten HICore 1 Safety-SoC

Automatisierungstechnikhersteller, die keine Risiken eingehen möchten, entscheiden sich für eine vorzertifizierte SoC-Plattform wie den HICore 1. Dessen sicherheitsgerichtete Funktionalitäten, z.B. die hochpräzisen 4-Quadranten-Zählereingänge, die sicheren IOs oder auch die sicheren PWM-Ausgänge, entsprechen allen Anforderungen der IEC 61508 (bis SIL 3) und der ISO 13849-1 bis PL e und Kat. 4. Aufgrund der Zertifizierung können sich Entwickler darauf verlassen, mit der gewählten Plattform ein Zertifikat nach ISO 13849-1 für ihr Produkt zu erreichen. Der Kunde spart sich hierdurch Aufwände für die Prüfung der Prozessorarchitektur. Hierdurch verkürzen sich der Entwicklungsprozess und damit die Zeit bis zur Marktreife stark. Darüber hinaus besteht die Möglichkeit, mit HICore 1 extrem platzsparende Designs zu verwirklichen. Die Architektur der SoC-Plattform mit zwei taktsynchronen Prozessoren erleichtert das Software-Design, da auf beiden Prozessorkernen des sicheren Systems der exakt selbe Code parallel ausgeführt wird. HICore lässt sich in einer Vielzahl von Safety-Anwendungen in der Fabrikautomation einsetzen,



von Sensorik über Aktuatorik bzw. Antriebstechnik bis hin zu Robotik oder fahrerlosen Transportsystemen.

Neben dem eigentlichen Produkt – bestehend aus HICore 1 SoC, vorzertifiziertem Betriebssystem und ausführlicher Dokumentation inklusive Safety Manual – sind Erfahrung und Kompetenz in der Funktionalen Sicherheit ein entscheidender Erfolgsfaktor bei der Entwicklung von Embedded Elektronik, die (mit dem Zielprodukt) auch nach der Norm ISO 13849-1 zertifiziert sein soll. Die zertifizierten Safety-Ingenieure von HIMA Embedded Solutions helfen dem Kunden auf Wunsch mit ihrer Erfahrung, die typischen Fallstricke bzgl. Zertifizierungsschwierigkeiten im Entwicklungsprozess zu vermeiden.

Die wichtigsten Vorteile des HICore 1 auf einen Blick

- **Verkürzte Time-to-Market:** Das ISO 13849-Zertifikat garantiert die Normenkonformität der Plattform, sodass Kunden keine Zeit in eine Eignungsprüfung investieren müssen. Auch die sehr aufwändige Nachweisführung (Test, Dokumentation, Berechnung der Performancewerte) entfällt.
- **Kostenersparnis:** HICore und zertifiziertes Betriebssystem bilden eine sicherheitsgerichtete Plattform, die den Entwicklungsaufwand stark reduziert, indem sie diesen auf die eigentliche Anwendung beschränkt.
- **Platzersparnis:** Minimaler Platzbedarf auf der Platine – mit der kompakten SoC-Lösung sind auch auf kleinstem Bauraum Lösungen bis zu SIL 3 / PL e realisierbar.
- **Zukunftsfähigkeit:** Mit HICore lassen sich Produkte nach aktueller Normenlage entsprechend der höchsten Sicherheitsanforderungen realisieren (SIL 3 / PL e). Werden die Sicherheitsnormen aktualisiert, ist die Chance höher, solche Produkte auch nach der neuen Version des Standards zertifizieren zu können und weiter zu vermarkten.
- **State-of-the-Art:** Der Kunde nutzt mit HICore eine Plattform nach dem „neuesten Stand der Technik" – dies kann im Schadensfall versicherungsrelevant sein.

Volle Flexibilität für Entwickler

Hard- und Softwareentwickler können das HICore 1 Safety-SoC samt qualifizierter Entwicklungsumgebung inklusive sicherem zertifizierten Betriebssystem und detaillierter Dokumentation erwerben. In diesem Fall führen Sie den Entwicklungs- und Zertifizierungsprozess selbst durch oder beauftragen die kompetenten Experten von HIMA mit der kompletten Umsetzung. Auch Co-Development, also eine gemeinsame Entwicklung mit dem Kunden, ist möglich.