Deploy a rich, Consolidated Industrial Controller while Managing Essential Safety Requirements

Industry 4.0 is creating the motivation and opportunity for businesses to modernize and digitalize their operational infrastructures. For years, businesses have installed systems that are physically separated based on their requirements for real-time, safety, and lower-criticality functions. While functional, this approach can be expensive due to costs related to implementation, maintenance, and reliability. Fortunately, these costs can be addressed by leveraging today’s advanced multicore system-on-chip (SoC) processors, complemented with the software technologies that enable the creation of complex, heterogeneous software architectures on these SoCs.

The Mentor® Embedded mixed safety-critical architecture provides an integrated solution that enables high-criticality functions to be consolidated with other functions on a single SoC. Manufacturers of industrial automation equipment can now develop control systems that deliver best-in-class functionality while shortening time to market, meeting safety requirements, and reducing downstream customer’s ongoing operational costs associated with their industrial infrastructure.

Mixed Safety Criticality on a Single SoC

Today’s system architectures utilize separate processors and separate systems to meet mission-critical requirements, including safety certification. As cost pressures mount, these components can be consolidated onto a single SoC. The low-overhead isolation features in Mentor’s solution enables a safety-critical system to be deployed alongside other systems on a single-core or multicore SoC with maximum resource efficiency. The technology enables high-criticality and low-criticality functionality to be mixed on the same system while maintaining strong separation between the two subsystems.

SOLUTION FEATURES:

- Mixed Safety Architecture: Utilizes Arm® TrustZone® to separate critical and non-critical domains
- Broad runtime options: Nucleus RTOS, Nucleus SafetyCert, Mentor Embedded Linux, Qt® Graphics
- IEC 61508 Certification: Incorporates Nucleus SafetyCert, certified for IEC 61508
- Industrial Connectivity Support: OPC UA, EtherNet/IP, EtherCAT, Data Distribution Service (DDS), and more
- Development & Optimization: Integrated development and system performance analysis tool

BENEFITS:

- Reduce risk
  Nucleus is market proven, having shipped in billions of products powered by hundreds of different types of MPUs/MCUs
- Faster time to market
  Integrated and tested modules from a single vendor speeds integration and application development
- Reduce costs
  Reduce size of safety-critical systems and use pre-certified components to reduce system certification costs; consolidate functions on the same SoC; reuse investments in general purpose OS, such as Linux, without additional safety risks; lower downstream customer costs related to reliability, power consumption, and maintenance
Mentor’s mixed-safety solution integrates the Nucleus® SafetyCert™ RTOS, which has been engineered for safety to meet the stringent requirements of IEC 61508, with other OS environments such as Mentor® Embedded Linux®. Nucleus SafetyCert enables a real-time, safety-certified programming environment that includes the Nucleus kernel, the Nucleus process model for space partitioning, runtime libraries, connectivity, networking, and data storage.

Reliability Requirements

Industrial systems require that certain standards of reliability and uptime are met. The operators of those systems must have the means to maintain visibility and control of the system at all times. The non-safety/non real-time components of the system are commonly addressed by a general purpose operating system such as Microsoft Windows, but increasingly Linux is being considered and adopted for these functions. These low-criticality parts of the system, which may be tolerant to some amount of downtime or failure, typically include a graphical operator panel for control and monitoring, and also for communication to the industrial control or information network layers for SCADA, operations, and MES functions. On the other hand, the real-time control, which could include safety-certified subsystems, is much less tolerant to aberrant or unexpected behavior. These high-criticality functions of the system must continue to run unaffected by whatever happens in the low-criticality functions of the system.

Mentor’s mixed-safety consolidated system leverages Arm® TrustZone® hardware technology to separate the system into a “Secure World” inside TrustZone, and a “Normal World” outside of TrustZone. By booting the Nucleus-based, high-criticality partition in Secure World, and subsequently loading the Linux-based, lower-criticality partition in the Normal World, the architecture ensures that if the lower-criticality system partition fails or requires rebooting, the high-criticality partition continues to function unaffected. The architecture also ensures that the graphics operator display continues to show status of critical systems as well as provide operator control even as the low-criticality partition remains non-functional, including the non-critical graphics and control.

Reducing Safety Certification Costs

Using pre-certified components such as the Nucleus SafetyCert RTOS, safety certification costs can be dramatically reduced. Because Mentor’s safety separation technology leverages the Arm® TrustZone® hardware separation mechanism, fewer lines of code in the system are required, which further reduces the cost of safety certification.

More About Mentor Embedded

Mentor’s Embedded Systems Division comprises the Mentor Embedded™ family of products and services, including embedded software IP, tools, and professional services to assist developers and silicon partners to optimize their products for design and cost efficiency.