TECHNICAL INSIGHT

Mixed-ASIL Data Distribution for Next-Gen SDV Architectures

Executive Summary

Automotive manufacturers developing Software-Defined Vehicles (SDVs) face a critical bottleneck: achieving ISO 26262 safety certification for complex, mixed-criticality data networks. Developing a custom, certifiable data distribution middleware typically demands thousands of engineering hours and delays time-to-market. By integrating RTI Connext® Cert as a pre-certified Safety Element out of Context (SEooC) under ISO 26262, engineering teams can save up to 12–18 months of middleware certification effort and eliminate millions of dollars in compliance overhead. This allows engineering resources to focus entirely on proprietary autonomous driving and vehicle control applications.

The Challenge: The Certification Bottleneck

Systems Architects for SDV platforms must manage massive, real-time data exchange across diverse vehicle domains — from Advanced Driver Assistance Systems (ADAS) and chassis control to infotainment. Automakers are responsible for the certification of application logic, operating system integration, network stack integration, and target hardware, as well as addressing safety at the system level.

As a zonal SDV architecture transitions from an R&D prototype to a production-ready platform, the engineering team must prepare the vehicle's communication layer for an ISO 26262 ASIL-D certification audit. Developing and demonstrating the safety of this data distribution backbone from scratch is highly resource-intensive. Every engineering hour dedicated to validating underlying middleware is time diverted from the core mission of developing differentiating autonomous driving algorithms.

The Solution: RTI Connext Cert as an SEooC

Rather than building a communication framework from the ground up, engineering teams can deploy RTI Connext Cert. Connext Cert is developed and certified as an SEooC, independently of specific end-user applications, target operating systems, and network stacks.

While Connext Cert provides the core infrastructure required to develop safety-critical software, it does not implement end-to-end safety functions by itself. Customers remain responsible for addressing safety at the system level, including hardware failures and their operational effects.

Defining the Certification Boundaries

To streamline the audit process, the team can utilize Connext Cert's clear delineation between the certified infrastructure provided by RTI and the customer-managed components.

Component Layer	Responsibility	Description
Platform-Independent DDS Library	**RTI — certified SEooC**	Fully-certified core data distribution library, accompanied by formal ISO 26262 SEooC certification and safety manual.
Application Logic	**Customer**	Application-specific functionality and safety rules.
OS Integration (Connext Cert OSAPI)	**Customer**	OS-dependent adapter code and the underlying operating system.
Network Stack (Connext Cert NETIO)	**Customer**	Network stack-dependent code and transport infrastructure.
Target Hardware	**Customer**	Microprocessor, microcontroller, and hardware platform execution environments.

Additional Considerations

System Architecture: Managing Mixed-ASIL Environments

In modern SDV architecture, safety-critical and non-safety functions with different ASIL levels frequently share compute and communication infrastructure, creating a mixed-ASIL environment. To prevent lower-criticality functions from interfering with higher-criticality functions, system architectures must incorporate robust Freedom From Interference (FFI) mechanisms.

Depending on the target architecture and safety requirements, these mechanisms may include:

- **Memory Isolation:** Software or hardware partitioning can isolate safety-critical functions from lower-criticality functions. Possible approaches include protected memory spaces, dedicated processor cores, or separate processors.
- **Timing Isolation:** Scheduling mechanisms and real-time operating system capabilities can ensure that safety-critical tasks receive sufficient execution time and meet required deadlines without unacceptable interference from other tasks.
- **Execution Protection:** Redundancy, error detection, and error correction mechanisms can be used where needed to prevent faults in one execution path from affecting safety-critical behavior.
- **Controlled Interfaces:** Clearly-defined and monitored interfaces between software components can help prevent unintended access, modification, or propagation of faults across component boundaries.

End-to-End Protection (EEP) & Zero Copy Considerations

To monitor data integrity during distribution across communication layers, architects leverage Connext Cert's End-to-End Protection (EEP) mechanisms, which align closely with AUTOSAR protection concepts.

This use strategically leverages EEP's core strengths in their safety case.

1. **Integrity vs. Correctness:** EEP automatically manages data integrity monitoring across the channel, freeing the team to focus on safely and certifiably integrating it at the communicating endpoints.
2. **Zero Copy Performance:** For high-bandwidth sensor data (such as LiDAR), the EEP mechanisms optimize for fast network throughput in situations in which Zero Copy via shared memory regions is not possible.

Business Impact

By leveraging the Connext Cert SEooC foundation, automotive manufacturers eliminate the need to build and independently certify their core platform-independent DDS library. While engineering teams remain fully responsible for certifying their specific application logic, network stack integration, and hardware, adopting Connext Cert as the data distribution foundation significantly reduces foundational middleware engineering. This strategic integration allows SDV engineering teams to focus on proprietary application development, accelerating the vehicle platform's path to system-wide ISO 26262 certification.

Connext Drive

Connext Cert is part of Connext Drive®. Download a free evaluation version of Connext Drive at evaluation.rti.com, to explore the latest features. Over 2 million vehicles now on the road run on Connext Drive.

ABOUT RTI

RTI is the real-time data streaming company for intelligent distributed systems. RTI Connext® software is the critical nervous system for over 2,000 designs across Aerospace and Defense, MedTech, Automotive, and Robotics.

RTI, Real-Time Innovations and the phrases "RTI Runs a Smarter World" and "Your systems. Working as one," are registered trademarks or trademarks of Real-Time Innovations, Inc.
All other trademarks used in this document are the property of their respective owners. ©2026 RTI. All rights reserved. TI-008 V1 1126

Your systems. Working as one.

CORPORATE HEADQUARTERS: 232 E. Java Drive, Sunnyvale, CA 94089 • +1 (408) 990-7400 • info@rti.com

rti.com rti.com/blog rti.com/podcast company/rti rti_software rtisoftware