Maintaining Critical Safety Standards in a Virtualized Environment

Understanding Design Assurance Requirements

WNDRVR

EXECUTIVE SUMMARY

Aircraft and autonomous platforms use systems with design assurance to ensure safety, enabling pilots to make accurate, split-second decisions and self-driving vehicles to navigate appropriately and on time. While safety-critical applications require different levels of assurance, applications that do not traditionally require safety assurance may also greatly benefit from it.

Wind River® and Mercury Systems have partnered with Intel® to develop a virtualized safety system that reduces the hardware footprint while maintaining the security and safety required to meet Design Assurance Level (DAL) requirements. With decades of experience in the industry, Wind River and Mercury Systems have delivered innovations that are paving the way for future applications based on artificial intelligence.

CONTENTS

SAFETY SYSTEMS ENHANCE SECURITY AND RELIABILITY

In the aerospace and defense industries, even in systems for which safety is noncritical, implementing a safety system provides notable benefits. Running a safety solution mitigates operational and security risks. A formal assurance process mitigates risk by ensuring that systems function correctly, with comprehensive failure detection and failure management.

A safety system also increases reliability, as the acceptable error rate is extremely low from the start. Built-in redundancy in the architecture and system ensures data integrity through formal hardware and software segregation.

Safety solutions such as those offered by Wind River and Mercury Systems offer the following key benefits:

ACHIEVEMENT OF INDUSTRY-STANDARD EQUIPMENT REQUIREMENTS

A rigorous, well-defined process for risk mitigation is applied throughout the different hardware and software components in every subsystem, determining the default DAL required for each by using guidelines in a safety assessment process.

The process uses hazard and fault tree analyses to examine the effects of a failure condition in the system. Failure conditions are categorized by their effects on the aircraft, crew, and passengers. Using the results of these analyses, a probability of failure for different subsystems is calculated and the appropriate DAL is applied to each subsystem, ranging from Level A, representing a catastrophic failure in which a total loss of life is likely, to Level E, in which there would be no effect on safety.

Level (% of Avionics sw*)	Failure Condition	Process Objectives	Code Coverage Required	System Failure Rate	Example System
Level A (35%)	Catastrophic (Maybe total loss off)	71	Level B + 100% of conditions (MCDC)	<1x10-9/flight hour	Flight Controls
Level B (30%)	Hazardous/Severe (Maybe some loss of life)	69	Level C + 100% of decisions	<1x10-7/flight hour	Level C + 100% of decisions
Level C (20%)	Major (May be serious injuries)	62	Level D + 100% of lines	<1x10-5/flight hour	Mission Computer
Level D (10%)	Minor (May be minor injuries)	26	100% of requirements	None	Video Switch
Level E (5%)	No Effect (No impact on passenger of aircraft safety)	0	None	None	Maintenance, Entertainment

Figure 1. Software Design Assurance Levels A–E

In the case of a large passenger aircraft such as a Boeing 787, a full formal certification with the FAA is required and critical. Wind River systems such as VxWorks® have not only been architected and built to meet the standards of DAL A but also can accommodate multiple DALs for different types of systems, to support multiple applications on the same compute platform.

> "The probability of failure needs to be incredibly low for passenger aircraft: one failure in a billion hours of flight. We're talking about much safer systems than we'd have in, for example, driving."
>
> *—Alex Wilson, Director of Business Development, A&D Market Segment Team, Wind River*

Platform Flexibility to Accommodate Safety on Multiple Levels

DAL certifications are not only limited to the air. An innovative idea to automate the towing vehicle used to take an aircraft on the ground to and from the runway was developed to save aviation fuel and streamline operations. Because the automated towing vehicle is a ground system, it was not immediately clear whether to follow avionics flight system or ground system guidelines. However, using VxWorks allowed the manufacturer the flexibility to apply a range of certification processes, and eventually the vehicle was certified according to avionics guidelines DO-178.

New Capability Validation to Support Autonomous Operation

Safety is important not only for controlling existing systems but also to innovate and introduce more system capability. In one example, introducing a high-performance computing platform by Mercury Systems for the Airbus A330 SMART MRTT Tanker aircraft Automatic Air-to-Air (A3R) refueling system added a much higher level of system complexity. Working toward full autonomous operation, Airbus, Wind River, and Mercury Systems were able to achieve full DAL-A certification for the A3R, as well as enhanced maintenance systems.

Safety Innovations for Emerging Technology

Traditionally, radar and sensor processing require a high-level processing unit using multiple processing components, making equipment difficult to certify. However, Mercury Systems recognizes the importance of developing a sensor with a safety pedigree, as technical advancements allow for more complex operations that depend on an extremely low error rate to secure the lives of pilots.

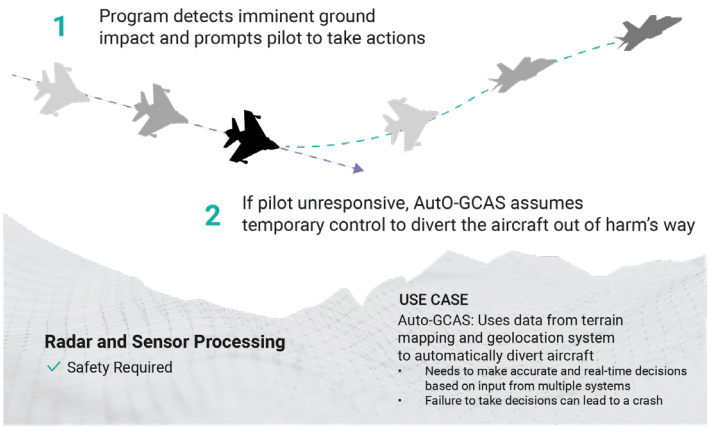


Figure 2. How innovations in radar technology impact safety requirements

THE PARTNERSHIP FOR A SAFETY VIRTUALIZATION PLATFORM

Systems are becoming much more complex, with more electronics and processing required to enable capabilities such as machine vision. These systems, in turn, integrate subsystems that must be guaranteed at the same high levels of safety and assurance. To achieve the technology and architecture required to build such complex safety systems, technology collaboration is required.

Mercury Systems has been a leading provider of open, modular, safe boards and systems for more than 30 years, focusing its civil and military space applications on safety design for both ground and airborne systems. Following the DO safety objectives of the Radio Technical Commission for Aeronautics (RTCA) and European Organisation for Civil Aviation Equipment (EUROCAE), Mercury Systems develops safe, rugged systems.

Today's applications require maintaining safety while providing high-speed, high-demand interaction between different types of processing elements. Fast and efficient communication is critical. The Mercury safety open computer platform is fully deterministic and includes multiple processors, including dedicated processors for graphics management. Isolated partitioning guarantees data integrity based on complete segregation in space and time, leveraging full mesh inter-processor (point-to-point) communication.

Mercury Systems worked in close partnership with Intel to develop a cutting-edge, first-to-market, Intel safety solution with both high-end processing capability and a strong safety pedigree. Incorporating operating system safety and compatibility into product requirements guarantees that the full system —including the military hardware — will be certifiable from the ground up.

Figure 3. Mercury Systems safety open computer platform

Having operated in the aerospace and defense industry for more than 40 years, Wind River is one of the market leaders within the embedded software world. The real-time Wind River Linux operating system is deployed in billions of devices across the aerospace, defense, industrial, and automotive industries. Within aerospace and defense, Wind River systems are used in air, ground, maritime, space, and cyber domains, with more than 550 safety certification projects based primarily on the DO-178C standard.

Wind River Studio offers cloud-native development, deployment, operations, and service of intelligent systems. Within Studio, Wind River Helix™ Virtualization Platform and VxWorks are key elements of the software architecture for avionic edge device safety.

In a virtualized system, high-performance computing platforms can be effectively segregated, allowing applications to run at different safety or security levels across the system. Using a virtualized approach allows mixing of different systems on the same platform while still mitigating the respective security risks and safety of each system.

Combining Helix Platform from Wind River and the high-end processor developed by Mercury Systems and Intel, functions can be safely and securely moved from multiple dedicated resources to fewer platforms. Using the Mercury Systems and Intel multi-core CPU allows the running of different operating systems, depending on the application required, while the Helix Platform uses the abstraction layers between different levels to mitigate safety and security risk, closely defining and controlling interactions between hardware and applications.

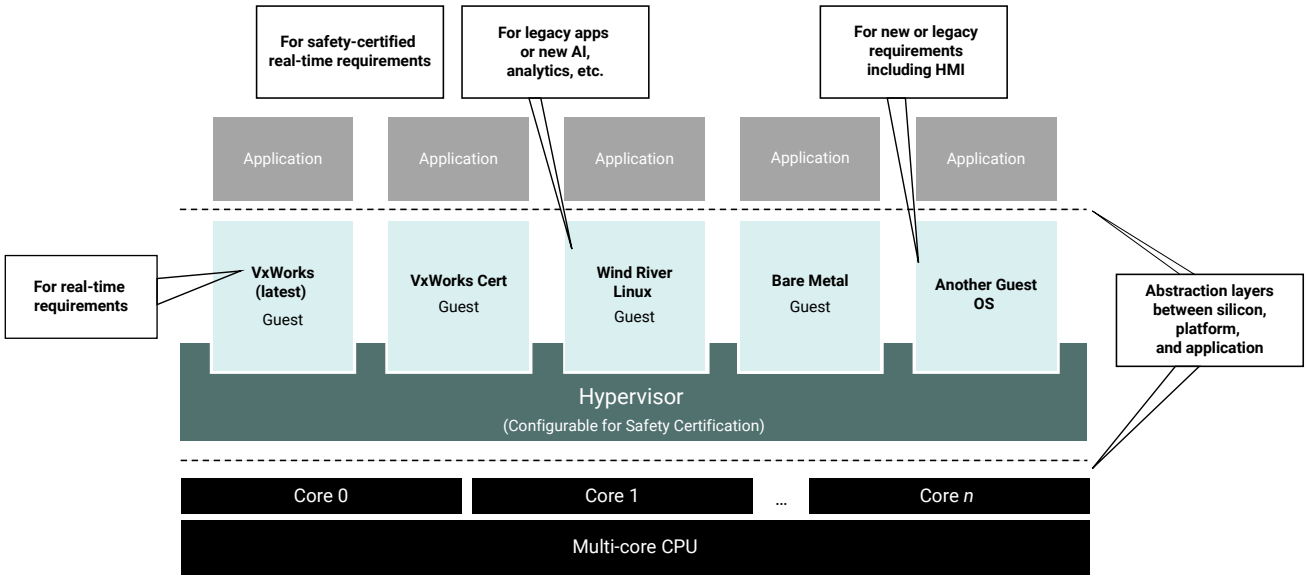


Figure 4. An example configuration of Wind River Helix Virtualization Platform

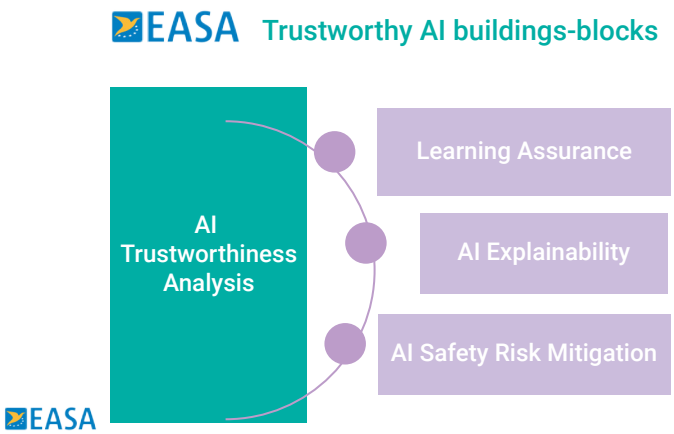
NEW CERTIFICATIONS FOR AI-DRIVEN SYSTEMS

Looking ahead, one of the most significant trends in the aerospace and defense industries is the move toward fully autonomous systems. In non-safety applications, autonomous aircraft are already flying to perform tasks such as the delivery of medical supplies and mineshaft mapping. However, introducing higher-level safety requirements, such as passenger flight, into autonomous aircraft requires advancement in both avionics safety technology and corresponding safety certification.

Urban air mobility systems such as air taxis, for example, rely on machine vision to replace pilots, leveraging cameras and sensors to sense and avoid obstacles, detect wires, and enable autonomous landing. These capabilities depend on powerful data processing and intelligent decision making, combined with enhanced radar and sensor processing, significantly increasing the complexity of fully certified safety systems.

To guarantee AI systems, bringing neural networks into a safety platform has only recently begun. The FAA has started publishing guidance on building a process to certify AI algorithms that depend on large volumes of captured data that need to be qualified and verified. A proposed process — the W-shaped process — is being developed to validate the productivity of trained neural networks when executing in an aircraft. Failure mode and effects analysis (FMEA) definitions for AI are still being scoped, with the goal of eventually bringing autonomous systems into full safety and security certification.

The AI trustworthiness framework



> "If you follow [the W-shaped process], you can build the proof of function. In this process, we focus on data set. As you may know, AI is data-hungry and uses large amounts of data, but going through your AI algorithm to mature it . . . ensures that these generalizations and other challenges are met."
>
> —*Yves Mathys, Mission Division VP Product Manager, Mercury Systems*

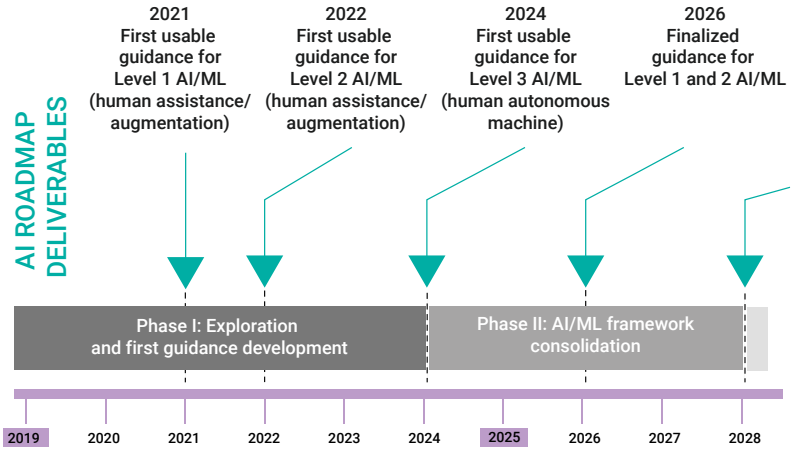


Figure 5. A roadmap for AI safety systems

CONCLUSION

For companies with significant safety software and safety systems experience, implementing innovative technologies, such as AI, into a system and navigating new requirements would likely be a top challenge when it comes to safety certification.

However, for companies new to the market that have not previously done safety certifications, a top challenge will likely be around how to set up the processes and functions within the company to meet the fairly rigorous safety standards requirements. In both cases, leveraging the expertise of Mercury Systems and Wind River in partnership can help validate safety architecture, systems requirements, and operational processes.

For more information, visit Wind River at www.windriver.com and Mercury Systems at www.mrcy.com.

WNDRVR

Wind River is a global leader of software for mission-critical intelligent systems. For 40 years, the company has been an innovator and pioneer, powering billions of devices and systems that require the highest levels of security, safety, and reliability. Wind River offers a comprehensive portfolio of software and expertise that are accelerating digital transformation across industries.