

WIND RIVER

Case Study: European Geostationary Navigation Overlay System

Safety-Critical System Powered by Wind River's VxWorks

Eur Ing Paul Parkinson

Senior Systems Architect, Aerospace and Defense, Wind River

Executive Summary

This case study describes the European Geostationary Navigation Overlay System (EGNOS) as well as the development by Logica of one of the most critical elements of EGNOS, the Integrity Processing Facility (IPF). The selection and deployment of Wind River's VxWorks real-time operating system (RTOS) for the safety-critical EGNOS IPF to fulfill Logica's design challenges are explained.

The U.S. GPS and Russian Global Orbiting Navigation Satellite System (GLONASS) provide positional accuracy of around 20 meters, which has enabled them to be used for a wide range of military and civil navigation purposes. However, this degree of accuracy is not suitable for safety-critical applications such as aircraft in-flight navigation and landing approach, or even ships navigating through narrow channels. As the skies, shipping lanes, and rail networks become increasingly crowded, high-precision satellite navigation systems are required to increase the capacity while maintaining safety, enabling efficient routing, minimizing energy consumption, and reducing carbon footprint.

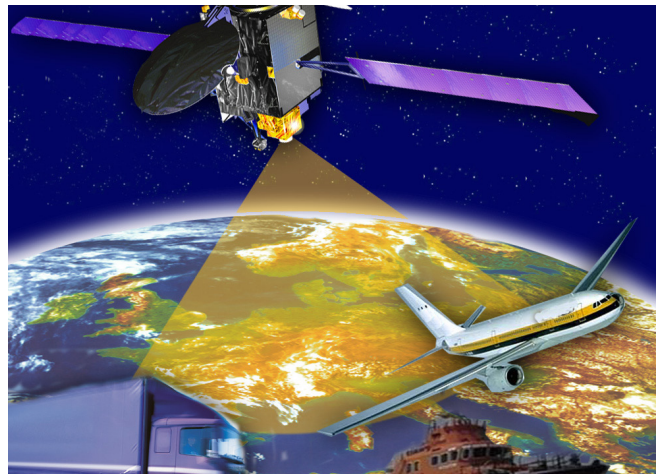
EGNOS is designed to improve the accuracy of existing military satellite navigation systems by making them suitable for safety-critical applications. It has been developed in Europe as a joint project between the European Space Agency (ESA), the European Commission (EC), and Eurocontrol and implements the first stage of the global navigation satellite system (GNSS). EGNOS is a precursor to Galileo, the full global satellite navigation system under development in Europe.

Designing for High-Integrity Operation

EGNOS consists of three geostationary satellites and a network of ground stations and transmits a signal containing information on the reliability and accuracy of the positioning signals sent out by GPS and GLONASS. It allows users in Europe and beyond to determine their positions to within 2 meters, compared to around 20 meters for GPS and GLONASS alone.

The three satellites consist of two Inmarsat-3 satellites, one over the eastern part of the Atlantic and one over the Indian Ocean, and the ESA Artemis satellite over Africa. These send out a ranging signal similar to that transmitted by the GPS and GLONASS satellites, except that the EGNOS signal is also modulated with integrity information about the position of each GPS and GLONASS satellite, the accuracy of their on-board atomic clocks, and information about disturbances within the ionosphere that might affect the accuracy of positioning measurements.

The EGNOS signal is actually calculated by a sophisticated ground segment comprising 34 ranging and integrity monitoring stations (RIMS) that measure the position of each EGNOS satellite and compare accurate measurements obtained from each GPS and GLONASS satellite. The ground segment determines the accuracy of GPS and GLONASS signals received at each station, and this information is incorporated into the EGNOS signal and broadcast to the EGNOS satellites via uplinks that transmit via transponders. The EGNOS Integrity Processing Facility (IPF) developed by Logica is the critical element that validates the information broadcast to safety-critical users.



EGNOS delivering a range of navigation services
© ESA

The Role of Software

The EGNOS IPF software processes the messages from RIMS, checks the validity of the messages prior to broadcast, and calculates the worst possible error if one satellite stopped transmitting. The EGNOS IPF must perform these checks to a high degree of accuracy and within hard real-time deadlines. In addition, because the output of the EGNOS IPF is relied upon in safety-critical applications, it must be safety certified to the joint avionics software safety standards RTCA DO-178B and EUROCAE ED-12B at Level B. This is where a failure condition is deemed by the standards to be “hazardous/severe” and could result in “some loss of life.”

Development Challenges

The EGNOS IPF project faced a number of significant development challenges because the system needed to perform processing in hard real-time using TCP/IP-based communication. In addition, the project was awarded in phases, with separate contracts for the development of the initial operating capability only supporting noncritical applications and for the safety certification of the system.

Challenge 1: Hard Real-Time Performance with TCP/IP Networking

The EGNOS IPF needs to meet hard real-time processing requirements and use TCP/IP networking. Logica wanted to undertake development of the EGNOS IPF using a proven hard RTOS and provide the ability to customize the networking capability to EGNOS’s specific requirements. Logica was able to achieve this using Wind River’s VxWorks RTOS and its configurable network stack. Logica was also able to perform analysis of the real-time behavior of the EGNOS IPF using Wind River System Viewer, which provided confirmation that the system was meeting its real-time requirements. Using this approach aided understanding of the real-time behavior of the system and enabled Logica to diagnose and debug problems more rapidly than through debugging alone.

Challenge 2: Lack of Available Hardware

During the development phase, the EGNOS IPF target hardware was not always available, but the developers needed to meet development milestone dates. Logica was able to exploit some of the unique capabilities of the Wind River development suite to provide increased productivity. In particular, it was able to use the VxWorks Simulator (VxSim), which simulates the behavior of the VxWorks kernel and APIs while running on a Windows or Solaris host platform, and continue functionality testing without target hardware, enabling Logica to meet its development milestones.

Challenge 3: Designing for Future Safety Certification

The development contract for the initial operating capability was only to support noncritical applications, and the contract

for the safety certification of the system was awarded separately by ESA. Therefore, Logica needed to undertake development of the EGNOS IPF using a hard real-time operating system with a clear path to safety certification that could be exploited in the second phase.

Logica undertook the development on VxWorks but restricted its applications use of VxWorks system calls to the safety-critical subset API. This enabled Logica to perform development, integration, and testing using VxWorks during the development phase and would enable it to rebuild its applications using the certified version of VxWorks during the safety-certification phase without having to change its application.

Challenge 4: Safety Certification on Dissimilar Processor Architectures

The EGNOS IPF also needed to meet system requirements for high availability, specifically when a single hardware failure would not interrupt the availability of the system. In order to meet this requirement, the EGNOS IPF uses a dual-redundant architecture with dissimilar processor architectures so that a single processor-level fault or error will not interrupt the availability of the system. VxWorks had already undergone safety certification on PowerPC processor architectures, but in order to meet the dissimilar processor architecture requirements, Wind River undertook the DO-178B safety-certification of VxWorks and DO-178B network stack on Intel IA-32 architecture.

Logica was then able to retest the EGNOS IPF to confirm that the functional operation was correct and the performance requirements were met. And Logica was able to incorporate the VxWorks DO-178B safety certification evidence into its system safety case for presentation to the certification authorities.

Project Achievements

Logica has developed a hard real-time system using TCP/IP networking in safety-critical systems, which has undergone safety certification and has been deployed successfully by ESA. This project illustrates very well how it is possible to conduct development and safety certification in a phased approach using commercial off-the-shelf (COTS) software. It also shows that by developing to the VxWorks safety-critical subset API, an application can be migrated to certifiable VxWorks without needing to be rewritten.

About the Author

Eur Ing Paul Parkinson is a senior systems architect with Wind River, working with customers in the aerospace and defense sectors in the UK and across EMEA. His professional interests include integrated modular avionics (IMA), Intelligence Surveillance Target Acquisition Reconnaissance (ISTAR) systems, and information security (InfoSec). He blogs on A&D industry issues on the Wind River website at <http://blogs.windriver.com/parkinson>.