Meeting LEO Satellite Systems Development Challenges with Simulation Technology

WNDRVR

EXECUTIVE SUMMARY

As the need for internet communications and connectivity increases in the everyday activities of the government and military as well as in commercial and personal interactions, satellite communication systems become a key to the future growth of communications. However, while the opportunities for and the importance of satellites grow, developers of low earth orbit (LEO) satellite constellations, ground stations, and terminals are facing major challenges in testing their systems to ensure successful operation, communication, and security.

Simulation technology provides a solution to these challenges that can save time, lower costs, provide valuable metrics, and improve performance and security.

Wind River® Simics® is a full-system simulator used by software developers to simulate the hardware of complex electronic systems such as LEO satellites. Simics allows on-demand and easy access to any target system, more efficient collaboration between developers, and more efficient and stable automation.

TABLE OF CONTENTS

TOP CHALLENGES

Satellite Technology Evolution Increases Cybersecurity Risks

Now, 65 years after the first man-made satellite was launched in 1957, there are more than 2,600 such satellites orbiting the Earth. Just over 70% of them are LEO satellites. LEO satellites are used by thousands of organizations around the world for communication, military reconnaissance, and other imaging applications.

As LEO satellite technology has increased in use and complexity, so have the challenges around increased cybersecurity risk, system update verification, multi-node analysis, and resource shortage management.

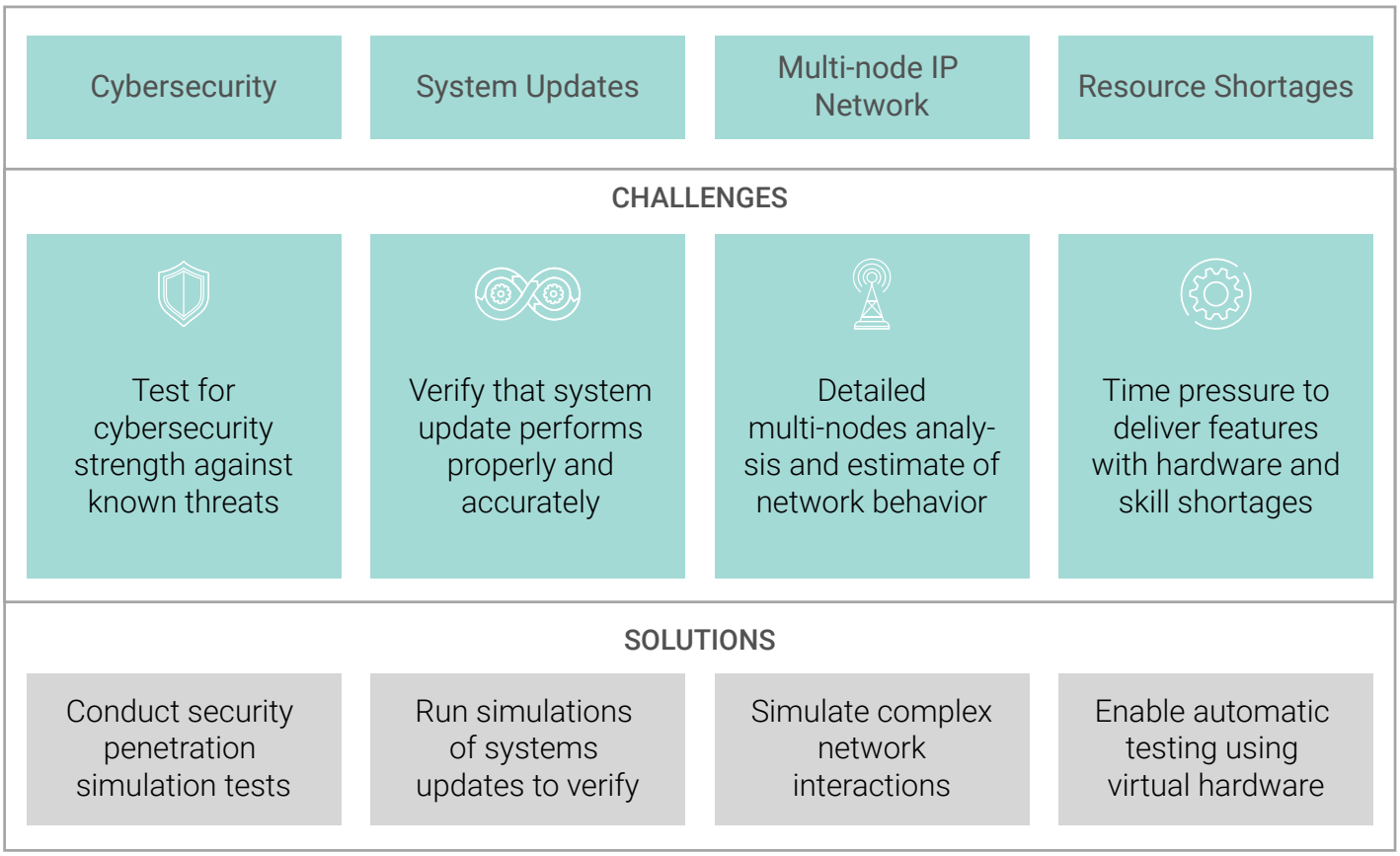

Figure 1. LEO satellite development challenges

Simulation addresses these challenges by allowing testing with increased frequency, which is often more cost-effective and provides feedback to developers to speed development with greater accuracy.

Looking specifically at cybersecurity, the significant amount of data being exchanged through daily satellite-based transactions — and the sensitivity and importance of this data — makes LEO satellites a high-value target for cyberthreats. That's in part because the lower-altitude orbiting LEO satellites are easier to access than MEO (medium earth orbit) and GEO (geostationary earth orbit) satellites.

Cyberattacks on satellites are executed to steal confidential or encrypted data, cause disruption to satellite operations, or corrupt or lock data for ransoming. This means that space organizations are increasingly facing significant security challenges as hackers threaten cyberattacks against space systems.

> "LEO satellite systems are a very high-value target for cyberthreats."
>
> *—Dr. James Hui, Senior Solutions Architect, Wind River*

Cyberattacks are evolving at a rapid pace, while legal and logistical restrictions sometimes prevent satellite makers from generating any updates, much less doing so at the rate required by the increasing threat landscape. Adding to the challenge is the way these complex systems are built, with components sourced from a wide range of suppliers, subcontractors, and manufacturers that rely on varying levels of security testing and risk mitigation.

Verification is critical to detecting vulnerabilities, remediating security issues, and building systems that mitigate risk and ensure security of satellites and other space systems. However, tracing every process and relationship that vendors rely on to verify and validate their products can be cost prohibitive. Testing the behavior of components, rather than the nuts and bolts of their composition and code, is one way around the onerous burden of tracing an entire supply chain. And testing in simulation not only allows developers to test behaviors of the entire system and its components but it determines cybersecurity vulnerabilities and provides an opportunity for remediation during the development cycle.

Software-Driven Design Requires New Update and Testing Approaches

Embedded devices — which typically run without the ability to update for a decade or more, due to the nature of their deployment — can lead to a "security debt" incurred by satellite manufacturers.

As satellite design has evolved to become more software-defined, satellites that can receive software and security updates while in service, using on-board AI capabilities to incorporate updates, learn, and interpret data, will be more efficient and autonomous.

Since the physical components cannot be made available to those working on software updates to a deployed satellite, developing and testing these updates in an abstracted environment, such as a simulator, is the necessary means to maintain satellite security and reduce risk of premature decommissioning.

Satellite Ops Testing Capabilities Apply to Multi-node Configurations

Most LEO satellites do not operate independently; rather, satellites function within complex, multi-node IP networks. Therefore, developing a new satellite requires taking into account its performance as part of a network. However, testing interaction between a pre-deployment satellite and other devices presents logistical challenges.

A simulated testing environment that allows modeling of more than one device facilitates interoperability testing to ensure effective and secure communication between satellites. As new communication methods are developed, these systems can likewise be incorporated into simulated environments to ensure functionality and improve cybersecurity.

Digital Twins Model and Verify Satellite Behavior

When working with complex technology such as satellite systems, testing software updates can be cost- and time-prohibitive. Simulation provides an alternative testing environment, using a digital twin by managing the model abstraction to preserve the relevant features of a satellite. This allows developers to verify behavior, detect vulnerabilities, and test failure conditions of software running on the satellite, without requiring access to the actual hardware.

Resource Shortages Exacerbate Risk and Performance Problems

The number and complexity of challenges in satellite design and operation, coupled with a hardware shortage and a limited number of skilled engineers, is driving the need for new approaches to testing and security, such as simulation, to meet the demands of increased speed of development and deployment.

For example, the Space Development Agency (SDA) plans to build several LEO constellations, the first of which includes 20 SDA satellites to be deployed in autumn 2022. The speed at which these initial 20 satellites were purchased, designed, built, and launched is significantly faster than that of conventional military satellites, while the cost was markedly less. While this is the result of an intentionally nonlinear, flexible, and agile approach to deployment, focused on meeting the needs of warfighters, it sacrificed security for speed, relying on communication links that are neither uniform nor secured to the standards required to ensure the integrity of the system.

Simulation can fill the gap when time and resource constraints cannot accommodate system testing on the physical satellite. Automating testing through scripts, combined with anytime-access to digital models from anywhere, supports agile development cycles and provides an avenue for security testing and risk mitigation pre-deployment.

SIMICS SIMULATION CAPABILITIES MEET TECHNOLOGY AND MARKET CHALLENGES

Simics is a simulation tool that uses a digital twin to perform deterministic virtualized hardware simulation. In a Simics simulation environment, multiple virtual hardware devices can be simulated, including communications on a virtual network. Each virtual hardware can run its own operating system as well as the application.

> "The simulation . . . is a digital twin of the satellite. There should be no difference in terms of what software to run — it should be the same software running on the simulation, so that you are exploring the actual features as well as trying to try to see underneath if there are any unintended bugs in your software in the simulation. [Simics] gives you another diagnostics perspective of the software before it is deployed onto the real satellite."
>
> —*Dr. James Hui, Senior Solutions Architect, Wind River*

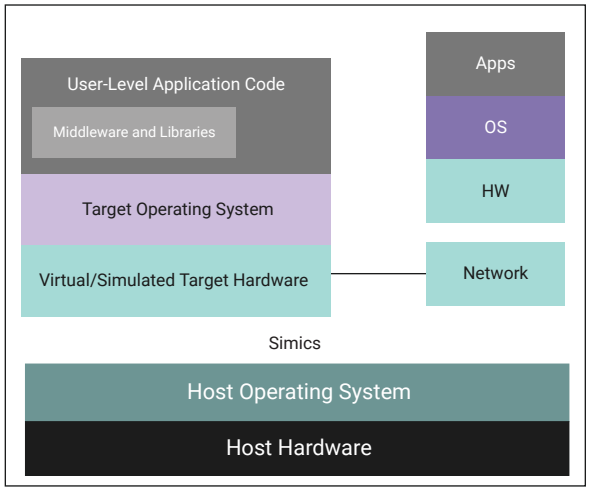

Figure 2. Simics enables deterministic virtualized hardware simulation

No specially compiled code is required to run on the Simics simulator. Simics accepts — and expects — the same production code that will be deployed onto real hardware, and it runs on any modern generic 64-bit PC with the Windows or Linux operating system installed. The simulator offers capabilities such as simulation of multiple systems, simulation scaling, scripting for repeatability, creation and restoration of checkpoints, and more. Simics is modular, allowing rapid device load and unload during runtime.

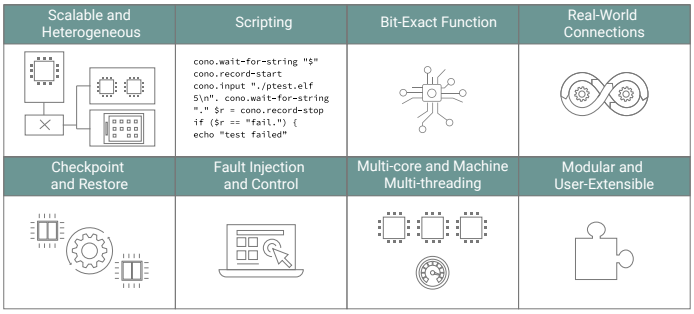

Figure 3. Simics system-level features

In addition, Simics is extendable to allow a mix of different technologies to be installed simultaneously in a single simulation environment. This allows developers to construct a big-picture simulation of how systems interconnect and behave with one another, rather than only analyzing one system in isolation. This includes use of other orbits such as NEO or GEO.

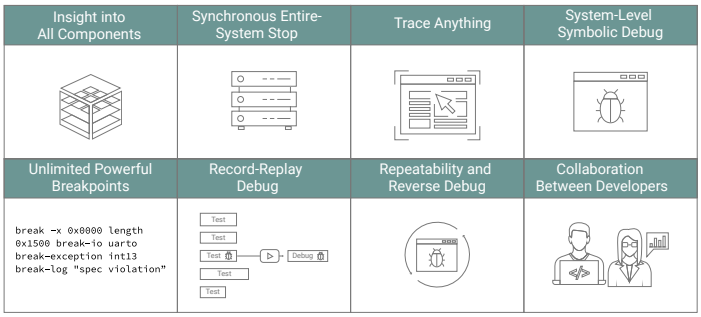

Figure 4. An example configuration of Wind River Helix Virtualization Platform

CONCLUSION

As satellite technology continues to advance, verification methods will need to keep pace with more complex requirements. In addition, the exponential increase in number of LEO satellites, specifically, along with their relatively close orbit, significantly expands the cybersecurity attack surface targeted by threat actors.

Full-system simulators such as Simics use a digital twin to simulate satellite hardware. Simics facilitates penetration testing to mitigate cybersecurity risks, supports update testing in abstraction before deploying to a remote target, enables multisystem modeling, and increases the speed of development using fewer human and financial resources.

To learn more, visit www.windriver.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.