Digital Twins Key to Cyber Resilient Infrastructure

Attack vectors in critical infrastructure are always changing, and agencies must move beyond just preventing cyber attacks and toward resiliency. Digital twin modeling can help governments prepare to work through any scenario.

December 16, 2022 • Tracy Gregorio, G2 Ops

Deploying systems fully designed to sustain operations during and after a cyber attack is quickly becoming the most realistic method for keeping critical infrastructure online.

Critical infrastructures often comprise complex systems of systems (SoS) running through interrelated IT platforms, applications, operational technologies (OT) and human/machine interfaces. We depend on systems of systems to orchestrate transportation networks, protect citizens from terrorist attacks and sustain utility grids. The increasing convergence of IT and OT systems creates opportunities for exploitation that can have catastrophic consequences.

Most state and local government IT managers have recognized these vulnerabilities and responded by installing multiple layers of cyber mitigation and prevention tools. But infrastructure reliability and availability are too important to simply rely on traditional perimeter controls, threat monitors and security patches. That's because these attacks are persistent, and bad actors continuously innovate new disruption techniques. The administration of layer upon layer of cybersecurity measures has become costly and complex with diminishing returns. Furthermore, those layers of cybersecurity can themselves unintentionally increase the surface area that threat actors can attack.

An important and often-overlooked variable is that the infrastructure to protect is not static. Changes occur at all levels, including obsolescence replacement, break/fix, functionality improvements and organic component updates. Having persistent sophisticated attacks against platforms with undocumented changes means it's difficult to ensure the core mission of the system is always protected.

This is where government executives and system managers need to move beyond prevention and toward resiliency. Cyber resiliency is a different kind of approach in which it is assumed we cannot count on cyber protections to keep 100 percent of attacks from impacting infrastructure. Those systems need to keep providing their crucial functions both during and after a successful attack. That means preparing to "work hurt" when an attack gets through: quickly detecting attacks, isolating bad actors that penetrated cyber defenses, ensuring critical services remain operational during an attack and rapidly reconstituting the infrastructure to baseline.

To aid resiliency of complex infrastructures, a new approach has been created through recent federal Small Business Innovation Research (SBIR) projects. The approach uses a methodology pairing digital twin modeling with the latest threat databases to help improve the design and operational resilience of SoS.

The first element of this approach is to use model-based system engineering (MBSE) techniques to create a digital twin for the SoS. The model includes devices, components, interfaces and data flows down to the specific device type and software release level. The digital twin then takes those IT and OT elements and models how critical operations across the infrastructure — network control and management, software updates, transfers between data lakes — flow through those components and subsystems.

The second element is to connect the digital twin models with cyber threat intelligence databases of the latest threats and attack vectors. Cyber analysts and IT managers can then continuously simulate how any known or emerging threat can impact the ability of their infrastructure to operate or continue performing its mission. Those simulations enable architects to deploy systems, plan updates and prioritize resources that make their operations less vulnerable and more resilient in the face of threat actors. And, when it's time for a major system upgrade, architects can better plan and build in attack resilience throughout the SoS design.

Using this proactive risk management approach, system architects can enable higher operational availability so that even when cyber attacks occur, the most important operations within critical infrastructures can keep running. Systems can be optimized to recover quickly from issues, application integrations can be protected, and automatic failovers or strategic backups can be optimized to ensure systems and key infrastructure functions continue uninterrupted.

Tracy Gregorio is CEO of G2 Ops, a woman-owned cybersecurity and IT engineering services company serving government and commercial enterprises. She chairs the Cybersecurity Committee of the Virginia Ship Repair Association and served on the Executive Committee of the Virginia Commonwealth Cyber Initiative. Gregorio earned an M.S. in Computer Science from Old Dominion and a B.S. from Virginia Tech.