**Lt Gen M. Unnikrishnan Nair**
Chairman
63SATS Cybertech

**PSU manufacturing is steadily moving toward connected, tech-enabled operations, increasing vulnerability to cyber threats across production and operational systems. Where is 63Sats seeing the most critical risks emerge, and how should leaders balance security with operational continuity?**

In PSU manufacturing, the advent of Operational Technology (OT) is creating new cyber risks. The most critical threats are ransomware attacks on industrial systems, vulnerabilities in legacy OT environments, supply chain exposures, and increasingly sophisticated AI-driven cyberattacks. Since many production systems were not originally designed with cybersecurity in mind, a successful breach can directly impact operations, safety, and business continuity.

Leaders must move beyond viewing cybersecurity for manufacturing as an IT function and adopt a cyber resilience mindset. The focus should be on continuous monitoring, AI-enabled threat detection, robust OT security, and incident preparedness. Security and operational continuity are not competing priorities, they must be built together to ensure resilient, uninterrupted operations.

**The shift toward smarter grids and digitally managed energy assets is expanding the cyber risk surface for PSU energy players. How is 63Sats helping secure these critical ecosystems, and which vulnerabilities require the most immediate focus to avoid system-level disruptions?**

The most immediate concerns for PSU energy players include vulnerabilities in OT environments, unsecured connected devices, third-party access points, increasingly sophisticated ransomware and nation-state attacks targeting critical infrastructure.

For PSU energy organizations, visibility across both IT and OT environments is critical. At 63SATS, we help secure ecosystems through a comprehensive cyber resilience approach that combines continuous monitoring, AI-driven threat detection, OT security assessments, vulnerability management, and incident response preparedness.

**Infrastructure projects today bring together multiple vendors, systems, and data flows creating complex interdependencies across execution. How is 63Sats securing such complex environments in PSU-led projects, and what should leaders prioritize to minimize disruption risks?**

Modern infrastructure projects rely on interconnected vendors, systems, and data flows that improve efficiency but also increase cyber risks. Vulnerabilities often arise through third-party access, supply chain dependencies, and inconsistent security controls across stakeholders.

Securing these environments requires a holistic approach that extends beyond organizational boundaries. PSU leaders should prioritize visibility across interconnected systems, robust third-party risk management, and security-by-design principles from the outset. The objective is not just to prevent cyber incidents, but to ensure critical projects remain resilient, operational, and on schedule despite an increasingly complex threat landscape. ■