

Secure Systems

Research Center

Zero trust end-to-end security
and resilience for cyber-physical
& autonomous systems

Innovation for a better world

The Secure Systems Research Center (SSRC) at the Technology Innovation Institute (TII) is pioneering zero-trust security, resilience, and safety for cyber-physical and autonomous systems using generative AI and large language models (LLMs). As autonomous technologies—such as unmanned drones, self-driving cars, automated warehouses, and smart city management—become increasingly integral across various industries, robust security measures are paramount. These systems offer transformative opportunities but also introduce unprecedented risks, especially in critical environments like nuclear power plants, industrial operations, and national defense.

Empowering the Future of Critical Infrastructure Security

SSRC's research focuses on developing zero-trust autonomous system platforms that adhere to the principle of “never trust, always verify.” By integrating generative AI and LLMs, they add intelligence to every part of the hardware, software, and communication stacks of autonomous systems. This integration enables the systems to manage their health, safeguard against cyber attacks, and adapt to make real-time decisions—essentially creating aware systems capable of self-management and threat mitigation.

Zero-Trust Autonomous System Platforms

In implementing continuous verification models, every device, user, and action undergoes rigorous authentication and authorization. Generative AI enhances this process by predicting potential vulnerabilities and automatically adjusting security protocols. By minimizing attack surfaces through techniques like micro-segmentation, combined with AI-driven threat detection, they significantly reduce vulnerabilities within systems. The center ensures resilient operations by isolating compromised components without affecting overall system functionality, with AI systems facilitating rapid detection and isolation of threats.

Leveraging open-source ecosystems such as RISC-V processors, PX4 Autopilot, ROS2/SROS, KVM/seL4 Hypervisor, NuttX Real-Time OS, and the TII/SSRC Modular Secure Stack, SSRC embeds security and resilience features into key components like robots, communication networks, and mobile platforms. The use of generative AI in these platforms allows for continuous learning and adaptation, enhancing the systems' ability to respond to new and evolving threats.





Zero Trust Mobile Platforms

In the realm of zero-trust mobile platforms, SSRC aims to deliver a complete secure software stack for mobile devices, robots (e.g., UxVs), and communicators within Mobile Adhoc Networks (MANET). They have developed innovative platforms like “Android-In-The-Cloud” and “Secure Labs and Secure Laptops,” which enable secure access to enterprise data on mobile phones and laptops without compromising user experience or corporate security. The integration of LLMs in these platforms provides advanced security features like anomaly detection and predictive analytics, enhancing the overall security posture.

Zero Trust Communications (Comms) Shield

The Zero Trust Communications (Comms) Shield provides secure and resilient communication over infrastructure-less environments, protecting against a wide array of security vulnerabilities and attacks such as de-authentication attacks, man-in-the-middle attacks, penetration attempts, routing attacks, flooding, and data exfiltration. By incorporating generative AI, the Comms Shield can intelligently adapt to changing environments and conditions, optimizing communication protocols in real time and enhancing resistance to sophisticated attacks. The AI-driven system can predict potential communication disruptions and reconfigure networks accordingly.

SSRC's technologies are network-agnostic, supporting Mesh, Long Range, LTE/5G, Satellite networks, and are being extended to support Wireless Sensor Networks. They contribute to open-source secure communication technologies, including BATMAN-adv routing improvements, open-source firmware, and their Synchronous Flooding transmission technology (OpenSTX under the Linux Foundation), which is incredibly useful for robot collaboration. Generative AI and LLMs play a crucial role in these contributions by enabling smarter, more efficient algorithms and protocols that can learn and improve over time.

Additionally, SSRC utilizes its technologies to enable secure wireless continuity for emergency access to backend services in critical situations like natural disasters where infrastructure is lost. The incorporation of AI allows for rapid deployment and configuration of communication networks in these scenarios, ensuring that essential services remain operational.

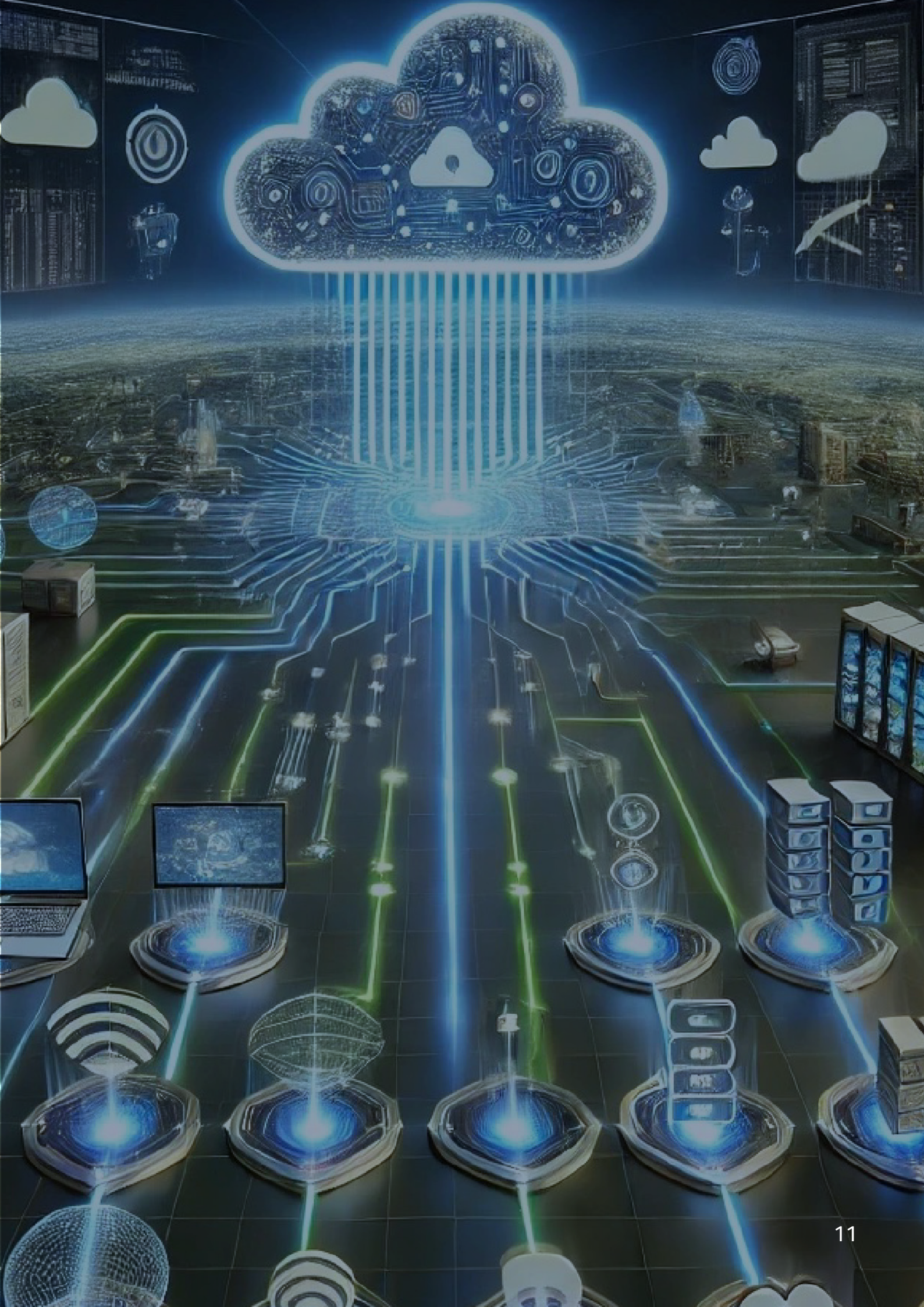


Pioneering Partnership, Inspiring Leadership

SSRC's research is accelerated through multiple partnerships and collaborations with leading academic institutions and research organizations across the Middle East, Europe, and the United States. These collaborations enable them to stay ahead of emerging threats and evolving technological landscapes by integrating the latest advancements in generative AI and LLMs. They are dedicated to pushing the boundaries of what's possible in autonomous system security, addressing critical challenges in sectors like defense, industrial automation, and smart city infrastructure, and building the future of secure, resilient autonomous operations.

Join Us in Shaping the Future

The Secure Systems Research Center invites potential partners, researchers, and stakeholders in critical infrastructure to join them in shaping the future of securing autonomous systems. By collaborating and innovating together—and harnessing the power of generative AI and LLMs—they aim to revolutionize the field by developing advanced security solutions that ensure the safe integration of autonomous technologies into society.



Innovation for a better world

TII helps build a better world by developing the most advanced, transformative technological innovations designed to benefit society. As a key component of the Abu Dhabi Government's Advanced Technology Research Council (ATRC), it promotes a culture of exploration with the aim of establishing Abu Dhabi and the UAE as an R&D hub and one of the next global leaders in breakthrough technology solutions.

For more information or to get involved, you can contact SSRC via their website at [www.tii.ae/ssrc](<https://www.tii.ae/ssrc>), email at [ssrc@tii.ae], or phone at .

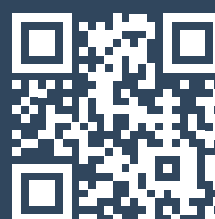


Secure Systems Research Center
Leading the way in Zero-Trust security for autonomous systems
through generative AI innovation.

Secure Systems Research Center



Technology Innovation Institute LLC
P.O. Box 9639
Abu Dhabi, UAE



tii.ae