iTrust Times

A Quarterly Newsletter

Issue Highlights:

Apr — Jun 2026 | Volume 12 Issue 2

From Centre Director's Desk

Dear readers,

Greetings from iTrust! Prof. Aditya Mathur, the founding centre director of iTrust, retired in June 2026. Since iTrust's inception in 2012, his vision, passion, and drive propelled iTrust into a world-leading research centre in cyber-physical system security. Under his bold stewardship, iTrust set up three world-class and unique CPS testbeds (SWaT, WaDi, EPIC), a feat never achieved before and have now become the cornerstone of CPS security in R&D, education, professional training, technology validation and cyber exercises. Because of his drive, iTrust has established strong partnerships with local government agencies as a trusted centre in helping Singapore to secure its critical infrastructure (CI). Look out for Aditya's interview with the CyberSG R&D Programme Office on his thoughts in cybersecurity innovations for CI protection.

On the research front, beyond Water and Energy sectors, Maritime is an emerging CI sector that continues to springboard iTrust to the next level. MariOT, the world's first industrial-grade shipboard OT testbed commissioned during the Singapore Maritime Week 2025 and certified by ClassNK, received the Minister's Innovation Award during the 2025/26 MOT Awards Ceremony for enhancing cybersecurity in the maritime sector. MariOT has also been used for maritime cybersecurity R&D, education, professional training, and for the first time this year, cyber exercises. During SMW 2026, two MoUs were signed: one among Singapore and Hamburg Port Authorities and IHLs to strengthen cooperation in maritime cybersecurity; another with ClassNK and Athena Dynamics to advance cyber resilience across maritime operations by leveraging the complementary strengths on research, classification expertise, and industry deployment. Two professional training programs on maritime cybersecurity, partnered with MPA, SSA, SIT and Singapore Poly, were also announced during SMW 2026. In May 2026, iTrust shared challenges and opportunities in securing critical infrastructure at the US-Singapore Workshop on Cybersecurity Innovation that was organised by the National Science Foundation and the Cyber Security Agency of Singapore (CSA) in Arlington, Virginia.

Cyber exercises have been one of the major activities in iTrust that leverage on our CPS testbeds. For the sixth consecutive year, iTrust proudly contributed to NATO CCDCOE's Locked Shields exercise as part of Singapore's Green Team, working closely alongside the Digital and Intelligence Service (DIS) and international partners. This year, iTrust is celebrating a major milestone: the 10th anniversary of CISS, a red-teaming cyber exercise, in collaboration with CSA and DIS.

Working in iTrust is a big responsibility, but at the same time it is also a great privilege and opportunity for those focused on CPS security. We are proud to have a professional team in iTrust, from cybersecurity technology engineers to project managers, who provide strong support to all the activities, from R&D to professional training and cyber exercises. We have excellent researchers who conduct cutting-edge research on CPS security, and welcome more passionate researchers to join iTrust. We are also grateful to the stakeholder agencies for their trust, encouragement and funding support to iTrust along the way. iTrust will continue to work hard to reach new heights in its next decade.

Jianying Zhou
Centre Director, iTrust, SUTD
Professor of Cyber Security, FIEEE

CSA SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

MOT Award

Minister's Innovation Award (Merit Award) 2026

We are proud to share that MariOT (Maritime Testbed of Shipboard Operational Technology) has been conferred the Minister's Innovation Award (Merit Award) at the 2025/26 Ministry of Transport (MOT) Awards Ceremony, in recognition of its contribution to strengthening cybersecurity in the maritime sector.

Developed as a world-first industrial-grade cyber-physical testbed, MariOT provides a safe and realistic environment for simulating shipboard operational technology systems and cyber threat scenarios. It enables maritime professionals, cybersecurity practitioners, and researchers to train, test, and validate cyber defence strategies without impacting real vessel operations.

By bridging the gap between theory and real-world application, MariOT enhances incident response readiness, accelerates cybersecurity innovation, and supports the development of more resilient maritime systems. It also serves as a collaborative platform for industry and academia to advance research and technology validation in maritime cybersecurity.

This recognition underscores the importance of continued innovation in safeguarding critical maritime infrastructure against evolving cyber threats.

CISS

Critical Infrastructure Security Showdown 2026

In collaboration with the Future Communications Research & Development Programme and CyberXCenter, we will include a 5G platform for the first time in CISS. In addition to the upgraded Electric Power and Intelligent Control (EPIC) power testbed, CISS will also include the Maritime testbed of shipboard Operational Technology (MariOT).

This year's theme is "**X Marks the Exploit**", inspired by Pirates of the Caribbean: The Curse of the Black Pearl. The story begins in the Caribbean, where the feared pirate ship, the Black Pearl, attacks the town of Port Royal.

The red team will take on the role of pirates seeking to retrieve a gold medallion from Port Royal, to lift the curse inflicted on the pirates. They will navigate the Black Pearl (MariOT) to the town of Port Royal and infiltrate the port's 5G network. As they penetrate deeper into the 5G core, they will discover that the gold medallion is secured within a vault powered by a nearby grid, EPIC.

After successfully attacking EPIC, disabling power to the vault and retrieving the gold medallion, the red team must make its escape in the cover of darkness. They will need to pivot back from EPIC to MariOT, regain control of the Black Pearl, and sail it out to sea. To complete the mission, they must also manipulate the vessel's systems to conceal its location and avoid detection.

For more information, visit: https://www.sutd.edu.sg/itrust/ciss-2026/

Locked Shields

Locked Shields 2026: Strengthening Global Cyber Defence Through Collaboration and Innovation

By: Sean Gunawan, Research Assistant, iTrust, and Jash Veragiwala, Cybersecurity Technology Engineer, iTrust

Organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Locked Shields is

the world's largest and most sophisticated live-fire cyber defence exercise. This year's exercise brought together cyber security professionals, military specialists, engineers, and industry experts from 42 participating nations to defend critical infrastructure against complex and fast-evolving cyber threats.

Held in Tallinn, Locked Shields 2026 featured 16 Blue Teams tasked with defending national-scale IT and Operational Technology (OT) environments against continuous and coordinated Red Team attacks. Beyond technical defence, teams were evaluated on strategic decision-making, legal and forensic analysis, incident response coordination, crisis communication, and the ability to maintain operational continuity during large-scale cyber incidents.

The exercise was conducted in two phases:

- The Partners Run, which focused on infrastructure validation, technical walkthroughs, and operational rehearsals
- The Main Execution phase, where participating teams operated under intense real-time attack scenarios.

For the sixth consecutive year, iTrust proudly contributed to the exercise as part of Singapore's Green Team, working closely alongside the Digital and Intelligence Service (DIS) and international partners to support the successful execution of the exercise. The collaboration reflected Singapore's continued commitment towards advancing cyber defence research and strengthening international partnerships in cyber security.

Fig 1.: Collaboration among iTrust, DIS, and NCL during Locked Shields 2026. (From left to right) Sean Gunawan, Research Assistant, iTrust; ME4 Tan Suan Zhi, DIS; Pek Chia Feng, Senior Security Analyst, DIS; Nagarajan Sivanadipatham, Research Associate, iTrust; Wei Wei, Software Engineer, NCL; Niklaus Kang, Infrastructure Assistant Manager, NCL.

This year, iTrust deployed a distributed version of its Secure Water Treatment (SWaT) digital twin integrated with a Siemens-based power grid environment, creating a highly realistic cyber-physical infrastructure scenario with real-world dependencies for participating teams. The integration of water treatment operations with power grid systems introduced an additional layer of operational complexity where failures in one sector can directly impact another, requiring Blue Teams to defend interconnected industrial processes while maintaining system stability, safety, and availability under active cyber-attacks.

Throughout the exercise, the Green Team managed demanding operational workloads, responded to infrastructure issues in real time, and supported participating Blue Teams as they defended their assigned systems. The scale and technical depth of LS26 required rapid debugging, efficient communication, and strong coordination across geographically distributed teams operating across multiple time zones.

Participation in Locked Shields 2026 also provided valuable opportunities for technical collaboration and professional exchange. Team members from iTrust worked closely with representatives from defence organisations, government agencies, research institutes, and international industry partners, gaining exposure to emerging cyber defence methodologies, large-scale cyber exercise orchestration, and resilience engineering for critical infrastructure systems.

At the conclusion of the exercise, participating teams reflected on the immense technical and operational challenges presented during LS26. The experience reinforced the importance of international cooperation, continuous innovation, and practical hands-on training in safeguarding critical digital infrastructure against future cyber conflicts.

MoU

Singapore and Hamburg Port Authorities and IHLs

During the Singapore Maritime Week (SMW) 2026, the Maritime and Port Authority of Singapore (MPA) signed a Memorandum of Understanding with the Hamburg Port Authority (HPA), the Singapore Institute of Technology (SIT), SUTD, the University of Hamburg (UHH), and the Hamburg University of Technology (TUHH), to strengthen cooperation in maritime

Fig 2.: Signatories, representatives and witnesses from Singapore and Hamburg Port Authorities and Singapore and Germany IHLs for the MoU signing on 21 Apr 2026 (Photo credit: MPA)

cybersecurity. This collaboration aims to develop technologies to strengthen cyber resilience in port operations and to support the exchange of cybersecurity best practices to enhance preparedness and incident response. SUTD's Maritime Testbed of Shipboard Operational Technology (MariOT) will be used to support joint research and development, cyber exercises as well as training with partners.

iTrust, ClassNK and Athena Dynamics

iTrust together with Japanese classification society, ClassNK – Nippon Kaiji Kyokai and cyber security consulting firm, Athena Dynamics Pte Ltd, signed a Memorandum of Understanding on 22 Apr 2026 to advance cyber resilience across maritime operations. This collaboration brings together complementary strengths: research depth and innovation, operational realism from industry deployment as well as regulatory and classification expertise.

Fig 3.: Prof Zhou Jianying, 2nd from left, with representatives from ClassNK and Athena Dynamics for the MoU signing on 22 Apr 2026

Events

Cyber Protection of Electric Harbour Crafts

To support Singapore's 2050 net-zero target, new harbourcrafts operating in Singapore's port waters will need to be fully electric, be capable of using B100 biofuel, or be compatible with net-zero fuels such as hydrogen. In Nov 2023, Yinson GreenTech (YGT) launched Singapore's first fully electric cargo vessel, the Hydromover. Two years on, an improved version, the Hydromover 2.0 was launched. Hydromover 2.0 "features improvements in range, faster charging time, higher payload capacity, and improved energy efficiency, along with a suite of advanced digital capabilities for smarter operations."

YGT is also cognizant of the suite of systems onboard its electric harbour crafts that require cyber protection to ensure safe vessel operation. Through the introduction of the Singapore Maritime Institute, YGT visited iTrust's Maritime Testbed of Shipboard Operational Technology (MariOT) to understand its capabilities and the cyber security risks faced by commercial vessels. YGT also extended an invitation for iTrust's maritime team to take the opportunity to visit both Hydromovers that were currently docked at the shipyard. The visit helped the researchers to appreciate maritime systems within an operational vessel, and the potential cyber risks these systems faced. At the conclusion of the visit, both parties were keen to collaborate through data exchange and the use of MariOT to demonstrate cyber risks and their mitigation measures.

Fig 4.: iTrust's maritime team with YGT hosts in front of the Hydromover 2.0

US-Singapore Workshop on Cybersecurity Innovation

In the 2022 press release by the Cyber Security Agency of Singapore (CSA) on the establishment of the United States-Singapore Cyber Dialogue, "Singapore and the US share deep mutual interests in enhancing cybersecurity cooperation, particularly as cybersecurity has become a key enabler for both countries to leverage the benefits of digitalisation to grow their economies and improve the lives of their people.

In the same spirit of cooperation, now on the R&D front, CSA and the US' National Science Foundation (NSF) organised a US-Singapore Workshop on Cybersecurity Innovation. The in-person workshop provided a platform for technical exchange between researchers from the US and Singapore, with the goal of building lasting and impactful collaborations in cybersecurity. Held over two days at Virginia Tech in Arlington, 40 participants from Singapore and the US engaged through keynote presentations, lightning talks, speed networking sessions, and roundtable discussions in topics ranging from AI (of course) to cyber

physical systems, IoT, privacy and wireless systems and communications.

Beyond cross-pollination of ideas and aware of each other's work, the workshop also seeded for joint projects whenever funding opportunities arise.

Fig 5.: Singapore and US participants at the conclusion of the workshop

Outreach

CypHER x SHE Learning Journey 2026

On 25 May 2026, CypHER, iTrust's outreach initiative for females in cybersecurity, in collaboration with SG Her Empowerment (SHE), organised a half-day outreach event designed to inspire and expose pre-tertiary girls to opportunities in the cybersecurity industry.

Fig Fig 6.: iTrust's Researchers and Engineers showcasing our testbed facilities to the participants. (Clockwise from Top left: Sean Gunawan, Research Assistant, iTrust; Aristotelis Mitsiou, Cybersecurity Software Engineer, iTrust; Dr. Anand Agrawal, Research Fellow, iTrust; and Andrew Tay, Cybersecurity Technology Engineer, iTrust.

The outreach event aimed to spark curiosity, broaden perspectives, and encourage greater female participation in the cybersecurity field. iTrust welcomed close to 60 girls and five teachers from five secondary schools, providing participants with firsthand insights into the work of iTrust researchers and engineers in safeguarding critical infrastructure cybersecurity. Through interactive testbed explorations, project sharing sessions, and a social media cybersecurity segment, participants gained a deeper understanding of real-world cybersecurity challenges and applications.

Featured on Media

From Our Partners: CyberSG Voices Featuring Prof. Aditya Mathur

In a recent episode of CyberSG Voices, our partners at CyberSG R&D Programme Office (CRPO) sat down with Prof. Aditya Mathur from iTrust to discuss cybersecurity innovations for critical infrastructure protection.

The episode covers the development of cloud-based solutions for critical infrastructure operators, the limitations of conventional IT security tools in operational technology environments, and emerging approaches to safeguarding essential services.

Click below to watch the full episode: **CyberSG Voices Episode 2: Critical Infrastructure Protection**

Scan to view previous issues of iTrust Times

General Enquiries

iTrust: *itrust*
NSoE: *nsoe_destsci*
CiMS: *cims*
Email addresses end with the domain ***@sutd.edu.sg***

Management

Prof. Jianying ZHOU
Centre Director
Professor, Information Systems Technology and Design (ISTD), SUTD
jianying_zhou

Prof. Aditya P MATHUR
Founding Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur

Mark GOH
Assistant Director, iTrust
mark_goh

iTrust Laboratories

Aanand R
Cyber Security Technology Engineer
aanand_r

Aristotelis MITSIOU
Cyber Security Software Engineer
aristotelis_mitsiou

Jash Jignesh VERAGIWALA
Cyber Security Technology Engineer
jash_veragiwala

Andrew TAY
Research Senior Technologist
andrew_taykongngee

Andy TAY
Education Lead
andy_tay

National Satellite of Excellence

Jillian CHIN
Senior Manager
jillian_chin

Angie NG
Manager
angie_ng

Vanessa LEE
Manager
vanessa_lee

Siti Nadhirah Shaik NASAIR
Deputy Manager
siti_nadhirah