

iTrust Times

Issue Highlights:

- ◆ DCS-CI 2026 *pg. 2*
- ◆ Water sector Collaboration *pg. 3*
- ◆ Visits *pg. 4*
- ◆ Workshop *pg. 4*
- ◆ OT Training *pg. 5*
- ◆ Conference Reflections *pg. 6*
- ◆ Featured on Media *pg. 7*

A Quarterly Newsletter



Jul — Sep 2026 | Volume 12 Issue 3

From Centre Director's Desk

Dear readers,
Greetings from iTrust!

The mission of iTrust is to secure the critical infrastructure via research and development, professional training, and cyber exercises. We built one-of-a-kind OT testbeds (SWaT, WaDi, EPIC, and MariOT) to provide safe and realistic platforms to support those activities. We also initiated a new OT cybersecurity forum (DCS-CI: Design of Cyber-Secure Critical Infrastructure) to facilitate conversations and collaborations among academia, industry, and government agencies to strengthen the security and resilience of the critical infrastructure.

iTrust and TWT jointly organized DCS-CI'26 in Buford, Georgia, USA. This is a unique forum that brings together researchers from academia, industry practitioners, and policymakers to discuss recent advances in strengthening the resilience of critical infrastructure systems. The cyber twin of a real water plant in Georgia developed by iTrust was also demonstrated at DCS-CI'26. DCS-CI will become iTrust new annual flagship event. DCS-CI'27 will be organized by iTrust in Singapore, with a focus on maritime cybersecurity. Participants will have the opportunity to do hands-on experiments on the world's first industrial-grade shipboard OT testbed MariOT. Stay tuned.

iTrust has been actively exploring the opportunities on various collaborations for maritime cybersecurity. During the trip for DCS-CI'26, iTrust delegates visited Georgia Tech hosted by Raheem Beyah, Saman Zonouz, and Wenke Lee. Their research on maritime cybersecurity was very impressive. iTrust also supported NUS Centre for International Law in successfully organizing a workshop on

strengthening maritime cybersecurity, not simply focusing on the technologies, but also from the perspectives of law, industry and regional cooperation. The tour to iTrust labs, especially the MariOT testbed, was highly appreciated by the workshop attendees.

iTrust just successfully concluded CISS'26, the 10th edition of Critical Infrastructure Security Showdown, jointly organized with DIS and supported by CSA. MariOT, EPIC and 5G testbeds were used in CISS'26. 10 out of 51 red teams entered into the finals. Each team had 4 hours to launch attacks. Congratulations to the top 3 red teams. They will share the \$10K cash prize. Detailed update will be shared in the next issue of iTrust Times.

iTrust hosted delegations from PUB led by Chief Executive, Mr Ong Tze-Ch'in, and CSA led by Deputy Chief Executive (Development) Mr Lee Shih Yen in August 2026. Both CSA and PUB are iTrust strategic stakeholders, and we appreciate their trust and support in R&D and technology translation for securing the critical infrastructure. iTrust also hosted the delegation from Japan led by Dr. Hisashi Matsumoto, Minister for Digital Transformation and Minister in charge of Cybersecurity. iTrust has a close collaboration with ClassNK on maritime cybersecurity. MariOT is the first maritime testbed being certified by ClassNK. We welcome more visitors to iTrust and seek opportunities for collaboration to secure the critical infrastructure.

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





Advancing Secure-by-Design for Critical Infrastructure



Fig 1.: iTrust Centre Director Prof Jianying Zhou giving the welcome address at DCS-CI 26

The International Conference on Design of Cyber-Secure Critical Infrastructure (DCS-CI 2026) was held from 2–3 September 2026 at The Water Tower in Buford, Georgia, USA. Jointly organised by iTrust, Singapore University of Technology and Design (SUTD), and The Water Tower (TWT), the two-day conference brought together researchers, industry practitioners, utility operators and government agencies to exchange ideas on strengthening the cybersecurity and resilience of critical infrastructure.



Fig 2.: Keynote address by Dr Selcuk Uluagac

Day One opened with a keynote by **Dr Selcuk Uluagac**, Program Director at the US National Science Foundation and Eminent Scholar Chaired Professor at Florida International University. In his keynote, “From AI for Cybersecurity to Cybersecurity for AI: An Evolving Threat and Research Landscape,” Dr Uluagac traced the changing relationship between AI and cyber security. While AI has long supported cyber defence through applications such as intrusion and anomaly detection, malware analysis and protection of cyber-physical systems, it is also increasingly becoming part

of the attack surface itself as it is embedded within autonomous, interconnected and safety-critical systems. His keynote highlighted emerging research opportunities at the intersection of AI, cybersecurity and resilient critical infrastructure.

DCS-CI received 30 submissions and accepted 9 papers (30% acceptance rate), and the proceedings are available from the conference web site at <https://dcs-ci.github.io/>.

These research presentations spanned diverse topics of ICS security, cyber-physical risk assessment, transportation and maritime cybersecurity, digital and cyber twins, privacy-preserving technologies and emerging threats involving AI. Among them, the **Best Paper Award** went to “Indirect Prompt Injection Against LLM Copilots in Industrial Control Systems,” authored and presented by **Salman Shahidand** and **Dilip Mallavrapu** (University of Alabama Birmingham).



Fig 3.: Andrew Ginter's presentation on islanding OT from IT

In line with the spirit of DCS as an academic-industry conference, participants also got to hear perspectives from industry and government. Andrew Ginter of Waterfall Security Solutions discussed how critical operations can continue even when OT systems need to be isolated from compromised IT environments. Min Kwang Lim from the Cyber Security Agency of Singapore presented Singapore's cybersecurity R&D vision towards 2030, with a focus on AI security, OT security, and quantum-safe technologies and a call for deeper international collaboration.



Fig 4.: Min Kwang Lim introducing Singapore's National Cybersecurity R&D Programme



Fig 5. (left to right): Stephen Reese (INL), Jeff Szabo (EPA), and William Siwiec (INL) gathering feedback on the capabilities of a planned water security test bed

Day Two kicked off with a brainstorming session by **Jeff Szabo**, EPA scientist, U.S. Environmental Protection Agency, **Stephen Reese**, Group Lead, and **William Siwiec**, ICS Cyber Security Engineer, Idaho National Laboratory on EPA and INL's collaborative efforts in designing a Water Security Test Bed (WSTB). Participants were invited to provide insights on future research priorities and test bed capabilities, such as the types of demonstrations and research that could be conducted, and opportunities for collaboration. Government representatives from CISA, FBI, and EPA also shared their roles and how they respond when a cyber incident occurs and offered tips on how companies can strengthen their cyber security posture through numerous channels and free resources.

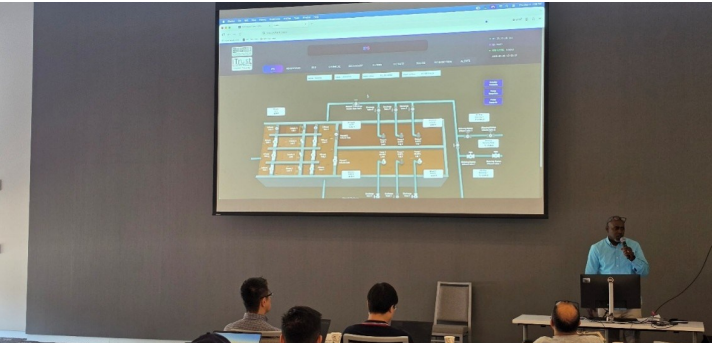


Fig 6.: Virgil Welch at a "live" demonstration of a cyber twin of a wastewater treatment plan

Virgil Welch, a Senior Water and Wastewater Specialist at TWT wrapped up DCS-CI 26 with a demonstration of a cyber twin – digital replica of a physical plant for cyber security use cases. The twin marks iTrust's **first ever cyber twin based on a real-world industrial plant** and represents an important milestone in its cyber twin journey. It was made possible through iTrust's strong and trusted collaboration with TWT, and its generous support and shared goal throughout the project. In developing the cyber twin, iTrust benefited from access and working knowledge to the plant's data, processes, and operational insights. This enabled iTrust to develop a cyber twin that is high fidelity and suitable for workplace training and cyber security preparedness. The success of this project is a concrete demonstration that a

trusted and supportive relationship between industry and academia can drive groundbreaking innovation and deliver real-world impact.



Fig 7.: iTrust Centre Director Prof Jianying Zhou announcing DCS-CI 2027

DCS-CI 2027 will be held in Singapore, with a focus on maritime cyber security. See you next year!

Collaboration

Collaborations in Water Sector: Visit by PUB and CSA

iTrust Centre Director Prof Jianying Zhou, Assoc Prof Daisuke Mashima and Research Fellow Dr Gauthama Raman hosted a delegation from Singapore's National Water Agency, PUB, led by its Chief Executive, Mr Ong Tze-Ch'in. In attendance was also the Cyber Security Agency of Singapore's (CSA) Deputy Chief Executive (Development) Mr Lee Shih Yen. Given iTrust's longstanding partnership with PUB, Dr Gauthama provided an overview of past and present collaborations with PUB, including translational efforts of iTrust's technologies AICrit and DAD with the help of a leading local cyber security company, Ensign InfoSecurity. Assoc Prof Daisuke then highlighted three main areas of focus in the next phase of iTrust's National Satellite of Excellence (NSoE) in Design Science and Technology for Secure Critical Infrastructure (DeST-SCI), a CSA-supported programme focusing on advancing the state of the art and state of practice in the design of secure and safe critical



Fig 8.: iTrust Centre Director Prof Jianying Zhou (far left) briefing PUB's Chief Executive Mr Ong Tze-Ch'in (fourth from left) and CSA's Deputy Chief Executive (Development) Mr Lee Shih Yen

infrastructure. Following a tour of the Secure Water Treatment and Water Distribution physical testbeds, the visitors were also shown demonstrations of iTrust's cyber twins – digital replicas of physical plants that are purpose-built for cyber security use cases.

Visits

Strengthening Japan-Singapore Collaboration in Critical Infrastructure

Cybersecurity

By: Assoc. Prof Daisuke Mashima, Information Systems Technology and Design (ISTD) and Academic Director (MTD Cybersecurity)



Fig 9.: A group photo with the delegates from Japan. (From left to right: Ms. Mayumi Yokoe, Digital Agency, Mr. Yukio Saita, National Cybersecurity Office, Dr. Hisashi Matsumoto, Minister for Digital Transformation, Prof. Daisuke Mashima, iTrust, Prof. Tony Quek, Associate Provost, Artificial Intelligence and Digital Innovation.)

International collaboration is essential to strengthening the security and resilience of critical infrastructure. iTrust was honoured with a visit by Dr. Hisashi Matsumoto, Minister for Digital Transformation and Minister in charge of Cybersecurity of Japan, together with delegates from the Digital Agency, Government of Japan, and the National Cybersecurity Office of Japan.

During the visit, Prof. Daisuke Mashima and the iTrust team shared our work in critical infrastructure cybersecurity R&D, OT cybersecurity training and exercises - including CISS, CIDeX, and NATO Locked Shields - as well as our OT cybersecurity testbeds covering power, water, and maritime systems. We also presented our work on cyber twins and interconnected testbeds designed to simulate cascading impacts across critical infrastructure.

The visit provided an opportunity for a valuable exchange on emerging cybersecurity challenges and international collaboration. Discussions also highlighted our collaboration with ClassNK, an international ship classification society in Japan, in maritime cybersecurity, and explored

opportunities to deepen cooperation between Japan and Singapore in OT security training and international capacity building.

Engagement with government representatives provides valuable insights into global trends, priorities, and emerging demands. We see strong potential for continued Japan-Singapore collaboration in advancing OT cybersecurity training, research, and international contributions to a more secure and resilient critical infrastructure ecosystem.

We sincerely thank Dr. Matsumoto and the visiting delegates, as well as the Embassy of Japan in Singapore, for taking the time to visit iTrust despite their busy schedule. We look forward to building on this international exchange and strengthening our collaboration in the years ahead.

Workshops

Strengthening Maritime Cybersecurity in Southeast Asia—CIL Workshop

iTrust was a supporting partner in the two-day workshop on “Strengthening Maritime Cybersecurity in Southeast Asia: Law, Industry and Regional Cooperation”. Organised by the Ocean Law and Policy Programme of the Centre for International Law (CIL), NUS, the workshop was held on 9 and 10 Sept 2026 at Orchard Hotel, Singapore.



Fig 10.: Group photo of workshop participants

More than 40 participants from national and international government agencies, maritime industries and academia attended the workshop to discuss emerging maritime cybersecurity challenges, exchange experiences and best practices across Southeast Asia.



Fig 11.: Prof Jianying Zhou delivering the welcome remarks



Fig 12.: Dr Awais Yousaf speaking on MASS code and Maritime Cybersecurity

On the 1st day of the workshop, iTrust Centre Director, Prof Jianying Zhou delivered the welcome remarks where he shared on the maritime cybersecurity activities done at iTrust. Dr Awais Yousaf, iTrust Senior Research Fellow, gave a presentation on “Maritime Autonomous Surface Ships (MASS): Cybersecurity Challenges”.



Fig 13.: Dr Awais Yousaf explaining to participants on MariOT



Fig 14.: iTrust Engineer, Aanand R giving a tour of SWaT

Participants witnessed first-hand iTrust’s maritime research work on the 2nd day. Prof Zhou gave a brief overview of iTrust, followed by a visit to the MariOT and SWaT testbeds.

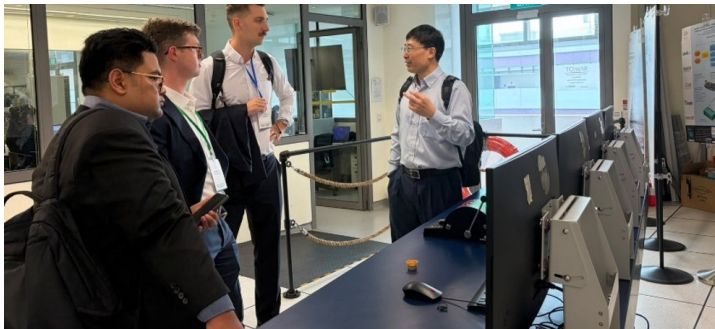


Fig 15.: Prof Jianying Zhou sharing the capabilities of MariOT

Trainings

Building Operational Technology (OT) Cybersecurity Capabilities

By: Aanand R, Cybersecurity Technology Engineer & Professional Training Lead and Dr Gauthama Raman M R, Senior Research Fellow



Fig 16.: Participants and trainers at the OT Cybersecurity Fundamentals course, SGInnovate event space, 16 July 2026. (In the front row, from left to right: Dr. Gauthama Raman M R, Senior Research Fellow, iTrust, Aanand R, Cyber Security Technology Engineer and Professional Training Lead, iTrust, Mr. Richard Wen, CEO of Three North Stars, Mr. Mark Goh, Assistant Director, iTrust, Andy Tay, Senior Research Assistant and Education Lead, iTrust)

On 16 July 2026, iTrust delivered a one-day OT Cybersecurity Fundamentals professional training course, in collaboration with Three North Stars, to 10 professionals from Singapore's public and private sectors at SGInnovate. Designed as a beginner-level introduction to OT and Industrial Control System (ICS) cybersecurity, the course combined foundational concepts with practical demonstrations and examples. Participants were introduced to OT/ICS architectures, the differences between IT and OT security, current threat actors and attack vectors, defence strategies, security standards including IEC 62443 and NIST SP 800-82, and the MITRE ATT&CK for ICS framework. A key feature of the programme was the use of iTrust's Cyber Twin technology to bring OT cybersecurity concepts to life. Through instructor-led demonstrations, participants observed normal industrial operations and simulated cyber-attacks, and examined changes in sensor, actuator and process behaviour. The demonstrations provided participants with an opportunity to connect cybersecurity concepts with their potential consequences on physical processes. The course was delivered by Aanand R, Cyber Security Technology Engineer and Professional Training Lead, and Dr Gauthama Raman M R, Senior Research Fellow, from iTrust, together with Richard Wen, CEO of Three North Stars. Andy Tay, Education Lead, and Mark Goh, Assistant Director, from iTrust also contributed practical insights drawn from their experience in OT security research. Drawing upon iTrust's expertise in OT cybersecurity research, engineering and

cyber-physical testbeds, the programme combined foundational knowledge with practical examples and demonstrations.

Post-course feedback was positive, with participants highlighting the live Cyber Twin attack demonstration, and case studies as memorable aspects of the programme. The practical demonstrations and cyber exercise were also well received for helping participants better understand OT cybersecurity concepts and their application in operational environments.

The course represents another step in the efforts of iTrust to translate its research and engineering capabilities into professional education, helping industry practitioners build a stronger understanding of the cybersecurity challenges facing increasingly connected OT environments.

iTrust also acknowledges the support of SGInnovate, the CyberSG R&D Programme Office (CRPO), and the Operational Technology Information Sharing and Analysis Centre (OT-ISAC) in making the programme possible.

Reflections

24th International Conference on Applied Cryptography and Network Security (ACNS) - Reflections

By: Alvin Chew, Student, MSc Security by Design

I am very grateful to the CSA-iTrust Masters Scholarship (CiMS) Programme for its strong support, which enabled me to attend and present my work at ACNS 2026. At the conference, I presented a workshop paper titled “TTNeural: A TFHE-Ready Lightweight Deep Learning Architecture for Encrypted Time-Series Analytics in Critical Infrastructures”, as well as a poster paper titled “Stage-Aware FHE/TFHE Co-Design for Confidential LLM and RAG Inference”.

The former is closely aligned with my current professional work in digital twin analytics, where I have been exploring how encrypted computation can be integrated into advanced engineering analytics for water networks and other critical infrastructure systems. At this early stage, the findings suggest that encrypted computation can strengthen the security layer for predictive analytics, while incurring only a modest loss in accuracy compared with fully plaintext analytics.

The latter poster paper is more closely connected to my intended academic research, possibly as part of future graduate study, where I hope to investigate the effectiveness of applying homomorphic encryption and its

variants to the computational framework of retrieval-augmented generation (RAG). Although this research remains nascent, I intend to continue exploring the problem during the final year of my current MSSD study at SUTD.

Overall, I am very grateful for the strong financial support from the CiMS Programme, which has enabled me to focus on my part-time studies while continuing to fulfil my full-time work commitments.

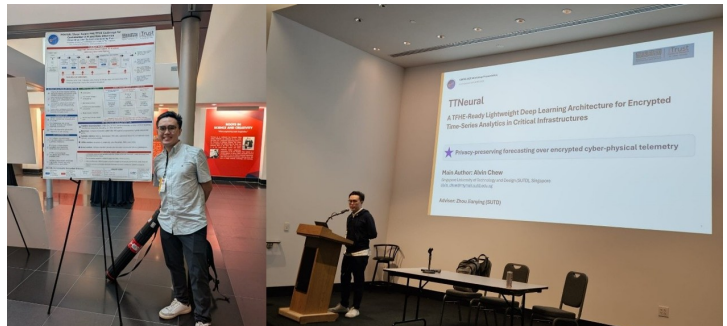


Fig 17.: Alvin Chew presented his research at the conference; showcasing his poster on “Stage-Aware FHE/TFHE Co-Design for Confidential LLM and RAG Inference” and presenting his work on “TTNeural: A TFHE-Ready Lightweight Deep Learning Architecture for Encrypted Time-Series Analytics in Critical Infrastructures.”

ACNS 2026: Where Cryptography Met Critical Infrastructure

By: Nadarajah Siyamraj (Raj), Student, MSc Security by Design

As nations increasingly depend on connected industrial systems for water, power, transport and telecommunications, cybersecurity research has become a matter of national resilience, not academic interest. That perspective sharpened for me at the 24th Applied Cryptography and Network Security (ACNS) conference at Stony Brook, New York, my first international conference after fifteen years in the field.

Across 59 papers, 11 sessions and 6 workshops, the programme traced a clear threat surface: IoT and IIoT intelligence, operational technology and critical infrastructure, AI security and safety, and private AI computation. The systems and network security track spoke most directly to Singapore's concerns, and two papers reframed how I think about our testbeds. ICSBoM, from Georgia Tech and NYU Abu Dhabi, showed why industrial patching so often fails: uptime pressures drive vendors to backport fixes inconsistently, leaving version numbers an unreliable guide to whether a device is exposed. Deception by Design, from Arizona State, offered a complementary answer. Its CDGym platform translates abstract deception strategies into automated, measurable experiments; against

eighty professional testers, adaptive deception meaningfully raised attacker costs where static honeypots did not.

Engaging with researchers of this caliber clarified the direction I want to pursue, network security by design, which I regard as central to protecting critical infrastructure and cyber-physical systems — the area I find most compelling. As an MSSD student, I hope to apply my experience to research that narrows the gap between theory and operational practice.

I have taken the first step by studying one paper in depth, Deception by Design, which I intend to develop into my future research. The gap between cryptographic theory and operational technology is where iTrust works, and where I hope to contribute.



Fig 18.: Closing of the informative event at Stony Brook University: 59 papers across three LNCS volumes, and six parallel workshops

MariOT provides a realistic environment for researchers and industry practitioners to investigate cybersecurity threats affecting shipboard systems. By combining real OT hardware, network infrastructure, simulation, emulation and hardware-in-the-loop capabilities, the testbed enables realistic cyberattack scenarios to be conducted safely on land.

Beyond research, MariOT serves as a platform for industry training and capability building, allowing maritime professionals to experience how cyber incidents can affect critical systems and practise detection and response in a controlled environment.

The platform is also evolving to support emerging maritime technologies, with future expansion into areas including cargo handling, maritime communications, autonomous and remotely operated vessels.

Through MariOT, iTrust is bridging the gap between cybersecurity research and real-world maritime operations, turning research into practical resilience for the ships of tomorrow.

Scan the QR code to
see MariOT in action:



Charting Safer Seas – Building Cyber Resilience for the Maritime Industry

The maritime industry is rapidly embracing connected and automated technologies, but greater connectivity also brings new cybersecurity risks.

Recognising the need to strengthen the resilience of maritime operational technology (OT), with support from the Maritime and Port Authority of Singapore (MPA) and the Singapore Maritime Institute, iTrust

engaged a vendor to design and construct the industrial-grade MariOT (Maritime Testbed of Shipboard Operational Technology).



Fig 19.: iTrust's MariOT Testbed: Navigational Bridge

General Enquiries

iTrust: [itrust](mailto:itrust@sutd.edu.sg)

NSoE: [nsoe_destsci](mailto:nsoe_destsci@sutd.edu.sg)

CiMS: [cims](mailto:cims@sutd.edu.sg)

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](mailto:jianying_zhou@sutd.edu.sg)

Prof. Aditya P MATHUR

Founding Centre Director, iTrust

Director, National Satellite of Excellence, DeST-SCI

Professor Emeritus, Computer Science, Purdue University

[aditya_mathur](mailto:aditya_mathur@sutd.edu.sg)

Mark GOH

Snr Associate Program Director, iTrust

[mark_goh](mailto:mark_goh@sutd.edu.sg)

Scan to view
previous issues of
iTrust Times



iTrust Laboratories

Aanand R

Cyber Security Technology Engineer

[aanand_r](mailto:aanand_r@sutd.edu.sg)

Aristotelis MITSIOU

Cyber Security Software Engineer

[aristotelis_mitsiou](mailto:aristotelis_mitsiou@sutd.edu.sg)

Jash Jignesh VERAGIWALA

Cyber Security Technology Engineer

[jash_veragiwala](mailto:jash_veragiwala@sutd.edu.sg)

Andrew TAY

Research Senior Technologist

[andrew_taykongngee](mailto:andrew_taykongngee@sutd.edu.sg)

Andy TAY

Education Lead

[andy_tay](mailto:andy_tay@sutd.edu.sg)

Mavis ANG Siew Ting

Cybersecurity Technology Engineer

[siewting_ang](mailto:siewting_ang@sutd.edu.sg)

National Satellite of Excellence

Jillian CHIN

Senior Manager

[jillian_chin](mailto:jillian_chin@sutd.edu.sg)

Angie NG

Manager

[angie_ng](mailto:angie_ng@sutd.edu.sg)

Vanessa LEE

Manager

[vanessa_lee](mailto:vanessa_lee@sutd.edu.sg)

Siti Nadhirah Shaik NASAIR

Deputy Manager

[siti_nadhirah](mailto:siti_nadhirah@sutd.edu.sg)



<https://sutd.edu.sg/itrust>



itrust@sutd.edu.sg



Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372