iTrust Times

A Quarterly Newsletter

Issue Highlights:

Oct — Dec 2025 | Volume 11 Issue 4

From Centre Director's Desk

Dear readers,

Happy New Year to all friends of iTrust!

First, I would like to thank the mentors, colleagues, students, and collaborators for the guidance and support along my career journey, which makes it possible for me to be elevated to IEEE Fellow for my contributions to applied cryptography and cyber-physical system security.

iTrust organised DCS-Water'25 jointly with TWT in Buford, Georgia, USA. This is a unique event that convened leading academics, industry practitioners, and utility operators to tackle the shared and emerging challenges in safeguarding water infrastructure from cyber threats. It also offered hands-on cybersecurity training in an interactive red-vs-blue team simulation. We will continue this practice to establish a unique forum on securing critical infrastructure.

iTrust has been working closely with industry partners on cybersecurity technology translation. I am delighted to share that iTrust has been awarded the CRPO grant to work with local security company Ensign InfoSecurity to develop a Cloud-based Intelligent OT-Centric Asset Monitoring for Critical Infrastructure.

iTrust is an active player in cyber exercises by leveraging on its unique OT testbeds. We organised the annual red-teaming cyber exercise CISS'25 jointly with DIS and attracted a record number of red teams from all over the world being involved - most of them being the first time to participate in CISS. We also supported DIS and CSA in organising the national blue-teaming cyber exercise CIDeX'25, to train and strengthen the capabilities of the 11 critical sectors to detect and deal with cyber threats to the IT and OT networks that control the operations of critical information infrastructure. iTrust contributed 3 OT systems for the water, energy and maritime sectors at CIDeX'25. Now iTrust is planning to support NATO CCDCOE's Locked Shields exercise 2026, which is the world's largest cyber defence exercise.

iTrust is making new progress on OT cybersecurity training and education. Recently our researchers conducted the first week-long pilot course on "Cybersecurity of Critical Infrastructure Twin" at Techno NJR Institute of Technology, India. We also hosted the interns from Tanglin Trust School to offer the OT cybersecurity training under the outreach programme designed for Year 12 and Year 13 students. With the commissioning of the new MariOT testbed, more training on maritime cybersecurity has been scheduled. We just completed training jointly with KPMG for the first batch of MPA VTM Officers, and are discussing with SIT and Singapore Polytechnic to offer new maritime cybersecurity training programmes.

I would also like to take this opportunity to welcome the new iTrust staff, Jash Jignesh Veragiwala and Aristotelis Mitsiou. We look forward to closer collaboration with partners from academia, industry and government agencies in the coming year, to strengthen the security and resilience of the critical infrastructure.

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

CSA SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

IEEE Recognition

Congratulations Prof Jianying Zhou!

We are delighted to announce that Professor Jianying Zhou, Centre Director of iTrust and Professor in the Information Systems Technology and Design (ISTD) pillar, has been elevated to the prestigious rank of **IEEE Fellow** in the IEEE Fellow Class of 2026. This honour is bestowed on no more than 0.1% of IEEE's voting membership annually, recognising individuals with outstanding contributions to engineering, science, and technology that have a significant impact on society. Prof Zhou's elevation to IEEE Fellow is in recognition of his seminal contributions to applied cryptography and cyber-physical system security.

iTrust extend our warmest congratulations to Prof Jianying Zhou on this well-deserved honour and look forward to his continued leadership in shaping the future of secure and trustworthy cyber-physical systems.

CyberSG Innovation Day 2025

CRPO Award—Translation and Innovation Grant

iTrust is a proud recipient of the **Translation and Innovation Grant** administered by the CyberSG Research & Development Programme Office (CRPO), funded by the Cyber Security Agency of Singapore under the National Cybersecurity R&D Programme. This grant continues the existing partnership between Ensign InfoSecurity and iTrust to develop a Cloud-based Intelligent OT-Centric Asset Monitoring for Critical Infrastructure.

With the current data fusion platform being developed using our advanced technologies, iTrust and Ensign is motivated to expand the innovation to a larger scale. The awarded project aims to address the critical need for scalable, intelligent monitoring solutions for large and complex critical infrastructure systems in Singapore. Combining iTrust's technologies and Ensign's commercialization expertise, the proposed system is designed to leverage plant design information and operational technology process data resulting in more precise and reliable anomaly detection. This project aspires to move a research innovation into real-world deployment, delivering faster, more reliable, and more secure anomaly detection solutions for critical infrastructure operators in Singapore and beyond.

Fig 1.: Mr. Tan Kiat How (left), the Senior Minister of State for the Ministry of Digital Development and Information, presenting the award to Mark Goh (middle), Assistant Director of iTrust and Dr Jonathan Goh (right), Head of Machine Learning at Ensign InfoSecurity.

DCS-Water 2025

Advancing Cyber Resilience in Water Utilities

By: Mark Goh, Assistant Director, iTrust

In the last week of October, iTrust and The Water Tower organised the second iteration of the **2nd International Conference on the Design of Cyber-Secure Water Plants (DCS-Water '25)** and an OT cyber defence training in the city of Buford, Georgia, USA. This two-day event gathered professionals in the water and wastewater treatment ecosystem to learn and share best practices to keep their utilities cyber safe.

DCS-Water '25

On Day 1, DCS-Water '25 convened leading academics, industry practitioners, and utility operators to tackle the shared and emerging challenges in safeguarding water and wastewater infrastructures from cyber threats. Setting the stage for DCS-Water '25 was Cole Dutton, a cybersecurity engineer with the U.S. Environmental Protection Agency, who talked about what it would take to cyber secure our water utilities, not least employing technologies but also capability development.

Drawing from his expertise in water distribution systems and years-long association with iTrust, Associate Professor Stefano Galleli's (Cornell University) morning keynote speech touched on the resilience, security, and the future of water systems. Prof Wenke Lee (Georgia Tech)'s afternoon keynote speech gave an overview of the threats that cyber-physical systems faced, drawing a link between the vulnerabilities of yesterday and the threats of today. Interspersed between the keynote speeches were presentations by various organisations and universities whose papers were accepted by the DCS review committee, with a particular emphasis on the use of AI in anomaly and intrusion detection in water treatment and distribution

systems.

Fig 2.: Prof Wenke Lee delivering his keynote

The afternoon programme comprised a "Singapore session" and invited speakers from the industry. In the Singapore session, Mr Zhihao Pang, Assistant Director from the Cyber Security Agency of Singapore, shared Singapore's efforts in building up cyber capabilities and resiliency through research and translational funding, and also invited collaborations across the international audience. Dr Jonathan Goh and Ms Pang Wen Ni from Ensign InfoSecurity demonstrated the ongoing work to translate iTrust anomaly detection technologies into a commercially-viable platform for anomaly detection in water utilities, complete with secured data ingestion for machine learning and an easy-to-understand UI as actionable intelligence for plant operators to make informed decisions. In a parallel work, iTrust Research Fellow Dr Gauthama Raman demonstrated his work using a cyber twin that was created out of the first two stages of a water utility plant in Gwinnett County, showcasing the strong trust and partnership between TWT and iTrust.

To round off the conference, invited industry speakers from cybersecurity firms (Armis, Global Solutions Group) and engineering firms (1898 & Co., Tetra Tech) gave their take on cyber security and resilience in water utilities, as well as showcasing their unique technological offerings.

Day 2 – Training: Cybersecurity in Practice for Water/ Wastewater Utilities

On the second day, attendees engaged in an OT-focused hands-on “Cybersecurity Training Experience” session at TWT. Led by iTrust Cyber Tech Lead, Siddhant Shrivastava Founding Centre Director Prof Aditya Mathur, the morning session focused on foundational OT cybersecurity concepts tailored for water and wastewater utilities. The curriculum was designed for participants with limited prior OT cyber background (operators, leadership, engineers) to build fluency in the cyber-physical threat domain and provided the segue into the afternoon session.

During the afternoon session, the attendees transitioned into an interactive red-vs-blue team simulation, where they were assumed the role of OT cyber defenders used tools like Wireshark to detect, respond, and recover from cyber-physical threats. iTrust’s water treatment cyber twin was used as the simulation platform, with the trainers launching cyber attacks. For many, this was the first time they were able to witness and appreciate the “physical anomalies” arising from a cyber attack in an environment they were familiar with (water utilities), and as one attendee summarised, “(the cyber twin) provided hands on experience on identifying attacks which is difficult to do in a live environment,” with another adding that “(it) was beneficial to develop a strategy for real, with my actual colleagues.”

Fig 3.: Attendees at the Cybersecurity Training Experience discussing attacks launched on the SWaT cyber twin

Post DCS-Water 2025 Call for Paper

The 2nd International Conference on the Design of Cyber-Secure Water Plants (DCS-Water’25), jointly organised by The Water Tower (TWT) and iTrust, was held successfully at TWT, Atlanta, Georgia, USA on 29 October 2025. It brought together leading minds from research, industry, and government to explore and exchange innovations in protecting water infrastructure from cyber threats.

As water and wastewater treatment plants grow increasingly digitised, they become more exposed to sophisticated and targeted cyberattacks. These facilities—essential to public health, economic activity, and environmental stability—rely on complex Industrial Control Systems (ICS), including PLCs, sensors, networked control platforms, and SCADA environments. While these technologies enable efficient and automated operations, they also introduce critical vulnerabilities that adversaries can exploit.

Cyberattacks on water infrastructure can result in far-reaching consequences, such as service disruptions, infrastructure damage, and compromised water quality. With the convergence of IT and OT systems, the growing scale of interconnectivity, and the evolving threat landscape, traditional perimeter-based defences are no longer sufficient.

Now it is open for a post-event call for papers. The accepted papers will be published by Springer in the same proceedings as for DCS-Water'25.

For more details, visit: https://itrust.sutd.edu.sg/post-dcs-water25-cfp/

Partnership Visits

Cyber "Seacurity": iTrust's Engagements with Fraunhofer Institutes in Germany

By: Mark Goh, Assistant Director, iTrust

In a series of research and partnership meetings held in Hamburg and Karlsruhe. Germany, Mark visited two of the Fraunhofer Institutes - the Centre for Maritime Logistics and Services (CML) in Hamburg and the Institute of Optronics, System Technologies and Image Exploitation (IOSB) in Karlsruhe. Prof Jianying Zhou, iTrust Centre Director, was also present in the discussions with CML. These visits will help to broaden iTrust's international cyber security collaborations in its latest venture into the maritime sector.

Fraunhofer FKIE and CML

On 15 Sep, we were hosted by Philipp Sedlmeier at CML in Hamburg, and he was joined by his colleagues from FKIE (Fraunhofer Institute for Communication, Information Processing and Ergonomics), Dr Jan Bauer, Konrad Wolsing, and Frederik Basels. After each respective institutes had introduced their work, the following areas of collaborations were identified:

- **Honeypots & Malware Analysis** – joint development of federated honeypot networks covering IoT and OT maritime devices, and shared malware datasets for automated labelling, classification, and attribution.
- **Firmware Vulnerability Analysis** – deployment of Fraunhofer's advanced firmware analysis tools in iTrust's testbeds for vulnerability detection and firmware lifecycle tracking.
- **Cyber Ranges & Simulation** – exploration of federated cyber-range capabilities by linking iTrust's and Fraunhofer's energy sector cyber twins and simulator
- **Maritime Cybersecurity Scenarios** – application of Fraunhofer's maritime bridge attack tools to iTrust's MariOT testbed to co-develop realistic cyber-exercise scenarios such as GPS spoofing and port communication attacks.
- **Intrusion and Anomaly Detection** – validate Fraunhofer's intrusion-detection systems during iTrust's annual Critical Infrastructure Security Showdown (CISS) red-teaming exercise

Fig 4.: Frederik Basels (right) demonstrating cyber attacks his lab's ship bridge system

Fraunhofer IOSB

At Fraunhofer IOSB on 16 Sep, Mark was hosted by its managing director Prof Jürgen Beyerer, Steffen Nicolai, and Christian Haas. The discussions centred on collaboration for cybersecurity of critical infrastructure and testbed federation to enhance realism and interoperability across international research facilities. Key areas of cooperation include:

- **Federated Testbeds and Cyber Twins** – linking physical testbeds and digital twins between IOSB and iTrust to support cyber exercises, dataset generation, and R&D use cases.
- **Tools Deployment** – deployment of IOSB's tools in vulnerability assessments of industrial automation components and asset-discovery within iTrust's operational testbeds.
- **Professional Training Exchange** – leveraging Fraunhofer's ISA-certified training programmes for delivery in Singapore, potentially augmented by iTrust's facilities via remote or hybrid modes.
- **Collaborative Research and Doctoral Projects** – combining IOSB's strengths in device fuzzing, industrial-protocol analysis, and anomaly detection with iTrust's expertise in dataset generation, cyber-twin engineering, and exercise design.
- **Mutual Access and Promotion** – reciprocal promotion and trial access to testbeds, enabling

Fraunhofer clients to evaluate iTrust's cyber-twin environments and fostering future joint publications and projects

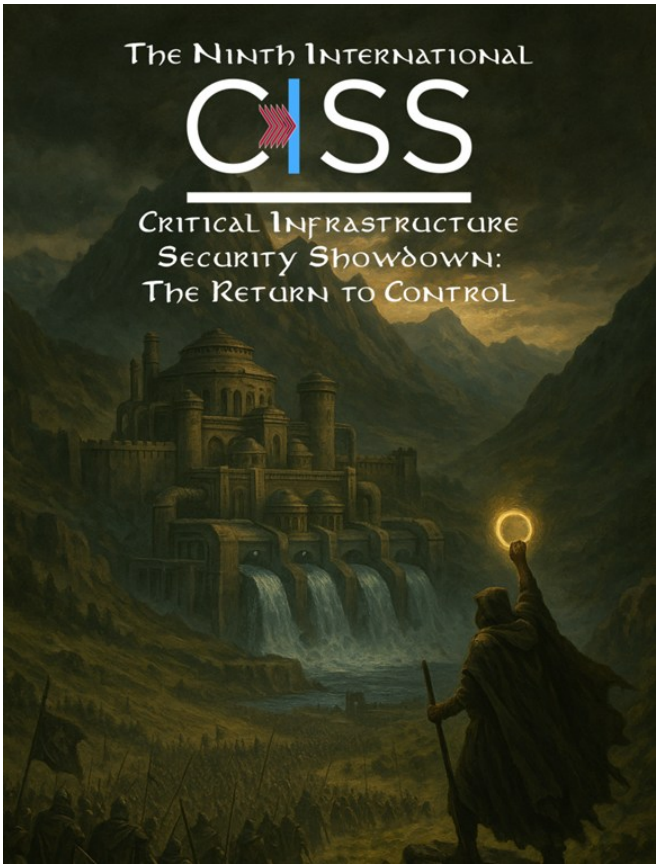
Fig 5.: IOSB showcasing its OT training platform capabilities

Within a month of visiting Dr Jan Bauer, and Frederik Basels in Hamburg, Prof Zhou and his team of maritime researchers had the delight of hosting them in iTrust. Research Fellows Drs Harishma Boyapally, Zeyu Yang and Awais Yousaf and Research Assistants Tirtho Sarker and Sean Gunawan each presented their respective work in IHO standards for data communication (Harishma), marine vessel intrusion detection methods (Zeyu), maritime cybersecurity risk assessment frameworks (Awais and Tirtho), and cyber exercises (Sean)

CISS 2025

Critical Infrastructure Security Showdown 2025

CISS 2025 is a premier and one-of-its-kind cyber exercise in operational technology. This international exercise is jointly organised by iTrust and The Digital Intelligence Service (DIS), and supported by the Cyber Security Agency of Singapore (CSA).



The 9th iteration of CISS started on 29 Sep with opening remarks by iTrust Centre Director Jianying Zhou and Commander, Cyber Protection Group, DIS, SLTC Benjamin Lim. returned to its familiar 2-stage format this year:

- 48-hour CTF-style Stage 1 with more than 60 challenges involving PLCs, digital twin, and a live scoreboard and a Finals with 4 hours of "live" testbed access
- In additional to SWaT, WaDi and EPIC testbeds, maritime and 5G assets were also featured
- A special OSINT brief by OT expert and iTrust's long-time friend and collaborator, Ms Marina Krotofil, so that the CISS finalists can be more targeted and better prepared
- Cyber security professionals from industry and academia as CISS Finals judges: Dragos, DIS, and National Cybersecurity R&D Laboratories
- Increased cash prize for top 3 finalists: S$5,000 / S$3,000 / S$2,000

Fig 6.: CISS organising team from DIS and iTrust, posing with CSA's Deputy Chief Executive Edward Chen (6th from left) and CISS partners from Dragos (Jackson Evans-Davies; 8th from right) and NCL (Yuancheng Liu, far right)

CISS 2025 is largest instalment of ever, with a flurry of activities spread across 7 days, beginning with a record number of 53 international red teams from 16 countries besting each other in a 48-hour Stage 1 OT-style CTF. Stage 1 culminated in 10 red teams emerging as top teams for CISS Finals, where they vied for conquest of the crown jewels of CISS - iTrust's four interconnected industrial-grade critical infrastructure testbeds. Even in its 9th iteration, CISS continues to attract new red teams, and this year saw nearly 80% of them participating in CISS for the first time. However, less familiarity did not necessarily mean less experience, and indeed, the top three red teams in the Finals - Laokoon Security GmbH and Deutsche Telekom Security GmbH (combined team; 2nd place), Munich University of Applied Sciences (1st place), and Standford Applied Cyber (3rd place) – were all first-time CISS participants.

iTrust also thanks its academia and industry partners in supporting CISS: CyberXCetnre, Dragos, Illinois Advanced Research Center at Singapore, National Cybersecurity R&D Laboratories, and Tallinn University of Technology, as well as the army of green team members who worked tirelessly behind the scenes to support the entire exercise.

CIDeX 2025

AI-Enabled Capabilities and Collaboration with Industry Elevate Defence of Critical Infrastructure at National Cyber Defence Exercise

This article is reproduced in full from Ministry of Defence, Singapore's website: https://mindef.gov.sg/news-and-events/latest-releases/12nov25-nr2/

Fig 7.: Participants from the DIS, Cyber Security Agency of Singapore and 11 Critical Information Infrastructure sectors at CIDeX 2025, held at the Singapore Institute of Technology (photo credit: MINDEF)

The Critical Infrastructure Defence Exercise (CIDeX), co-organised by the Digital and Intelligence Service (DIS) and the Cyber Security Agency of Singapore (CSA) is being held from 11 to 14 November at the Singapore Institute of Technology. Minister for Defence Mr Chan Chun Sing and Minister for Digital Development and Information Mrs Josephine Teo visited the exercise site today. During the visit, they were briefed on the conduct of CIDeX 2025 and on how CIDeX strengthens inter-agency collaboration to detect and tackle cyber security threats. Ministers also observed demonstration of tools developed in-house by the Singapore Armed Forces' Cyber Defence Test and Evaluation Centre.

CIDeX focused on training and strengthening the capabilities of the 11 critical sectors to detect and deal with cyber threats to Information Technology (IT) and Operational Technology (OT) networks that control the operations of Critical Information Infrastructure (CII). The exercise is supported by iTrust, Singapore University of Technology and Design (SUTD) and the National Cybersecurity Research & Development Laboratory. CIDeX is part of the National Cyber Exercise Programme, which is driven by the CSA.

CIDeX 2025 involves over 250 participants from the DIS, CSA and 33 other organisations, and for the first time, participation from all 11 CII sectors. During the exercise, participants from the Blue Teams, comprising representatives from participating organisations, defended their respective digital infrastructure against live simulated cyber-attacks launched by a composite exercise planning and control team made up of CSA, DIS, Defence Science and Technology Agency, GovTech, IMDA and LTA personnel. Exercise scenarios involved attacks on both the IT networks and testbeds that aim to disrupt operations, such as compromising a 5G network, and disrupting power supply and rail operations. This year's exercise scenarios were developed with the use of an Artificial Intelligence (AI) tool, which provided suggested attack pathways to engineer potential attack scenarios and intrusion vectors. These scenarios were further built on and refined by the planning and control team to shape realistic simulations that mimic attacks by malicious threat actors.

Private sector partners including Singtel, and global technology companies such as AWS, Check Point Software Technologies, Dragos, Fortinet, Google Cloud and Splunk (a CISCO company) were closely involved in the exercise preparations. They provided input on the cyber-attack scenarios, enhancing the simulated attacks' realism for higher learning value for the participants, and contributed training expertise to the six-day hands-on training programme prior to the exercise, to develop and hone participants' cyber defence competencies.

On the sidelines of CIDeX 2025, the DIS and SUTD also launched the Cyber5G testbed. Built with telco-grade components, the Cyber5G testbed allows academia and operational partners to conduct threat modelling and cyber training for the telecommunications sector. The testbed enables research on real-world attack vectors that threaten national infrastructure, for the development of robust defensive and mitigation strategies.

CIDeX 2025 provided participants with the opportunity to sharpen their instincts and technical competencies and share expertise and perspectives across organisations. Commander Defence Cyber Command/Defence Cyber Chief Colonel Clarence Cai said, "As national cyber defenders, we are also embracing the use of AI to enhance cyber defence, in keeping pace with global cyber threats. In collaboration with our cyber partners, the SAF is developing cyber-AI experimentation and operationalisation

capabilities to apply transformative innovations to cyber defence. These capabilities elevate our operations and deploy the expertise of our skilled cyber talent and national servicemen where it matters the most."

Deputy Chief Executive (National Cyber Resilience) Edward Chen of CSA said, "Cyber threats to Singapore are real, complex, and rapidly evolving. Large-scale exercises like CIDeX give our defenders the realistic training to hone their craft and stay ahead of increasingly sophisticated cyber threat actors. We are appreciative of this strong partnership with the SAF to build Singapore's collective cyber resilience."

Training & Development

Tanglin Trust School Outreach

In October 2025, iTrust welcomed students from Tanglin Trust School as part of the Institute at Tanglin's outreach programme designed for Year 12 and Year 13 students. This marked iTrust's first collaboration with an international school where our programme introduced students to a broad range of cybersecurity fields, including network security, OT security, and penetration testing.

To help students understand the Cyber Kill Chain, each participant worked with two Virtual Machines (VMs): one acting as the adversary and the other as the victim. Using these VMs, they carried out realistic attack scenarios on their own host machines and learnt to use tools such as Metasploit to compromise the victim system.

The programme covered both IT and OT security. Students were introduced to key cybersecurity frameworks, including MITRE ATT&CK and the Cyber Kill Chain, which outlines the seven stages of an attack: Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.

Fig 8.: Andy (far left) and Aanand (far right) pictured with their students from Tanglin Trust School.

The training began with network security fundamentals, where students learnt how devices connect, how to interpret network topology, and how to determine whether devices are in the same subnet. With this foundation, they progressed to hands-on exercises using penetration-testing tools provided by iTrust to simulate adversaries infiltrating an Engineering Workstation (EWS) within a water treatment plant network.

After obtaining access, students performed reconnaissance to understand their position in the network and confirm whether they had reached the OT environment. They then moved into the OT security component, where they learnt how the water treatment process operates. This enabled them to execute controlled OT attack scenarios safely and effectively.

We are pleased to work with Tanglin Trust School in introducing OT focused skills in aspiring cybersecurity professionals and welcome the students to join iTrust as undergraduate interns in years to come.

OT training in Techno India NJR Institute of Technology, India

By: Shrivastava Siddhant, Cyber Tech Lead, iTrust

In November 2025, iTrust researchers Siddhant Shrivastava, Nagarajan Sivanadipatham, and Dr Revati Govind Godase conducted a week-long pilot course on "Cybersecurity of Critical Infrastructure Twin" at Techno NJR Institute of Technology, Udaipur, using the SWaT water treatment and SHOCK power cyber twins to train students in securing real-world industrial control systems.

Fig 9.: Instructors from iTrust and Participants from Techno NJR Institute of Technology pictured in front of NJR campus in Udaipur during the November 2025 pilot course.

The intensive 5-day program blended OT/ICS security

fundamentals with hands-on labs in Python-based historian analysis, OT network traffic inspection for ENIP/CIP, IEC61850, and OPC-UA, as well as controlled cyber-physical attacks and invariant-based detection on the twins. Active learning was reinforced through frequent Kahoot quizzes, team-based exercises, and a NATO CCDCOE-style purple-teaming cyber exercise, culminating in penetration testing reports that assessed both technical and documentation skills; the course received exceptionally strong feedback and laid the groundwork for deeper collaboration with Indian institutions.

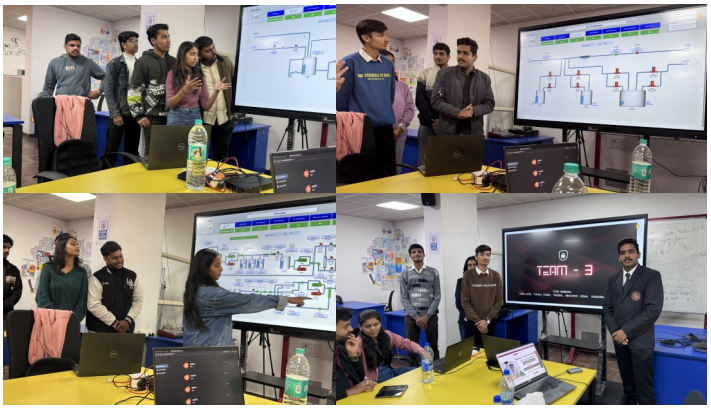


Fig 10.: Team-based presentations by the participants from NJR Institute of Technology.

Students particularly valued the opportunity to work directly with industry-grade cyber-physical testbeds remotely hosted at iTrust, gaining exposure to end-to-end workflows from reconnaissance and attack execution to detection engineering and incident reporting in a realistic but safe environment. The pilot also featured a dedicated "train-the-trainer" module for faculty and technical staff, designed to support local adoption of the curriculum and the potential deployment of twin-based laboratories in India, thereby extending the impact of iTrust's research, education, and outreach agenda in critical infrastructure cybersecurity.

New iTrust Staff

Jash Veragiwala

graduated with a Bachelor's degree in Computer Science and Design with a minor in Artificial Intelligence from the Singapore University of Technology and Design (SUTD).

Prior to joining iTrust, he gained experience in software development and AI projects through internships, where he worked on mobile applications, AI-powered chatbots, and augmented reality training toolkits. His work involved close collaboration with industry partners to design and deliver innovative digital solutions.

Outside of work, Jash is passionate about sports. He enjoys playing cricket, basketball, and table tennis, and is always eager to pick up new games and stay active.

Aristotelis Mitsiou

joins iTrust with a background in software development and data engineering. He holds a Master's degree in Computer Science with specialisation in Computing from the National University of Singapore, as well as a Bachelor's degree in Computer Science from the University of Nottingham.

In addition to his professional experience as a data engineer, Aristotelis brings valuable customer support and technical training expertise from his previous role on a support and training team. He is also passionate about personal software projects and game development. For more than 10 years, he has been an Add-on Developer for ProMods, a team behind one of the most popular modifications for Euro Truck Simulator 2. He recently earned the title of Specialist in recognition of his deep knowledge of truck cabin accessories and vehicle licence plates.

Outside of work, Aristotelis enjoys travelling and exploring different cultures and cuisines. He also keeps up with the latest developments in the automotive and aviation industries and often relaxes through car-spotting and plane-spotting.

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

Siddhant Shrivastava
Cyber Tech Lead
shrivastava_siddhant

Andy TAY
Education Lead
andy_tay

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

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

Scan to view previous issues of iTrust Times

https://itrust.sutd.edu.sg
itrust@sutd.edu.sg
Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372