# iTrust Times

## A Quarterly Newsletter

### Issue Highlights:



**Apr —Jun 2025 | Volume 11 Issue 2**

## From Centre Director's Desk

Dear readers,

Greetings from iTrust!

It is the 10th year anniversary for iTrust Times, a quarterly newsletter providing the update of iTrust activities and achievements. From this issue onwards, we will only publish our newsletter on the iTrust website, without printing out hardcopies anymore.

Cyber exercises on OT systems is one of the core activities in iTrust. iTrust has been involved in NATO Locked Shield (LS) exercise since 2021. LS25 marked the 15th anniversary of the world's largest and most technically advanced live-fire cyber defence exercise that brought together more than 4,000 cyber defenders from 40 nations. Again, iTrust formed a Green Team responsible for the design, deployment, and maintenance of SWaT cyber twin in LS25. iTrust also participated with DIS as a Red Team conducting sophisticated cyber-attacks against the simulated infrastructure. Thanks to Siddhant and Aanand for their contribution to LS25. We are delighted to receive the letter of commendation from CCDCOE in recognition of iTrust's contributions to the success of LS25. iTrust is also organizing the annual CISS exercise. This is an excellent opportunity for Red Teams to pit their skills and knowledge in a one-of-a-kind OT red teaming cyber exercise that utilises iTrust interconnected industrial-grade OT testbeds as its platform. Interested teams can register before 1 July 2025. The qualified teams will enter the finals in the week of 29 September. The top 3 red teams will receive the awards. iTrust always welcomes collaborations with research organizations, industry partners and government agencies on OT cybersecurity. iTrust signed MoU on maritime cybersecurity with TalTech and CR14 from Estonia, together with MPA and SMI. They were involved in the cyber exercise using our new MariOT testbed during Singapore Maritime Week in March 2025. Daisuke visited a couple of universities in USA together with CSA in March 2025. Some potential collaborations are in discussion with Carnegie Mellon University, New York University, Virginia Tech, and University of Pittsburgh. iTrust is working with CSA to train next generation of cybersecurity professionals by offering prestigious CiMS scholarship to MSSD students. Five CiMS scholars were funded to attend ACNS 2025 in Munich. This gives them a good learning experience in listening to the talks by the leading cybersecurity researchers from all over the world and interacting with them which will be very helpful for their future career. iTrust is planning for the next phase of development. We are working closely with CSA and the relevant stakeholders on the research directions to address the real-world cybersecurity problems and the new sectors of critical infrastructure to be explored. We will put more efforts on the translation of new OT cybersecurity technologies to create bigger impact in the real world.

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

CISS 2025

## International Critical Infrastructure Security Showdown (CISS) 2025

iTrust invites cyber professionals to participate in the 9th iteration of the International Critical Infrastructure Security Showdown (CISS) 2025 as a Red Team. CISS is co-organised by iTrust and the Digital and Intelligence Service, and in partnership with the National Cybersecurity R&D Laboratories at the National University of Singapore. This is an excellent opportunity for Red Teams to pit their skills and knowledge in a one-of-a-kind OT red teaming cyber exercise that utilises interconnected industrial-grade OT testbeds as its platform.


CISS 2025 returns with a familiar modality and added features:

- Two-stage competition: Qualifying Round (48-hour CTF) + Finals: "Live" testbed access (4 hours)
- CTF challenge contributions by more local and international collaborators
- Hybrid platforms: OT physical testbeds and cyber twins
- Mystery platform
- Live scoreboard
- No cap on number of teams per organisation, though each team will still be limited to 8 persons
- Increased cash prize for top 3 finalists: S$5,000 / S$3,000 / S$2,000

Important dates:

- Qualifying Round:
  - From 29 Jul 2025, 0900h to 31 Jul 2025, 0900h (SGT, GMT+8)
  - Briefing to Red Teams will be held on 23 Jul 2025, 1100h (SGT, GMT+8)
- Finals:
  - From 29 Sep 2025 (Mon), 0900h to 3 Oct 2025 (Fri), 1800h. Each Red Team will have dedicated a 4-hour slot to launch their attacks on the testbeds
  - Briefing will be held on 29 Aug 2025 1600h (SGT, GMT+8)

CISS is a fully remote cyber exercise. Interested teams can register their interest here before 20 Jul 2025 or via the QR code below. There is no cost to registering and participating in CISS.


DCS-Water 2025

## Design of Cyber-Secure Water Plants 2025 (DCS-Water 2025)

Our Jointly organized by iTrust, Centre for Research in Cyber Security at the Singapore University of Technology and Design (SUTD) and The Water Tower, the 2nd International Conference on the Design of Cyber-Secure Water Plants (DCS-Water '25) brings together global experts to address the urgent and growing cybersecurity challenges in water and wastewater infrastructure.


As smart water systems become more integrated and digitally connected, defending them from cyber threats

is no longer optional; it is essential. DCS-Water '25 offers a rare opportunity to learn from leaders in the field and gain hands-on experience with real-world cyber defense tools and strategies.


Date: October 28–30, 2025

Venue: The Water Tower campus, 2500 Clean Water Court, Buford, GA

Important dates:

- ◊ Full paper deadline: August 5, 2025
- ◊ Abstract deadline: September 30, 2025

SMW 2025

## Poster Presentation at Singapore Maritime Week 2025

*By: Dr. Awais Yousaf, Research Fellow, iTrust*

Our team of maritime researchers recently participated in the Singapore Maritime Research Conference (SMRC) 2025, where they presented two research posters highlighting our recently inaugurated maritime cybersecurity testbed, MariOT and latest research work in the domain of maritime cybersecurity risk assessment. The first poster, titled "Maritime Cybersecurity Risk Assessment Framework for Next Generation Vessels," was presented by Dr. Awais Yousaf. It introduced a structured approach to evaluating cyber risks in modern, digitally integrated autonomous vessels. Dr. Awais Yousaf explained FMECA-ATT&CK-ATLAS (FAA) framework for cybersecurity risk assessment to attendees of SMRC 2025 and engaged in discussion sessions.

The second poster, "MariOT: A Maritime of Shipboard OT Systems for Cybersecurity Research, Training, Exercise and Education," was presented by Dr. Zeyu Yang. This work showcased our innovative MariOT platform, designed to support hands-on cybersecurity research, training, education, exercises, technology validation and testing in maritime operational technology environments.

The conference was a rewarding experience. Our researchers had the opportunity to engage with a diverse audience, and we had numerous discussions with the many attendees who visited our posters. The experience was both enriching and motivating, reinforcing our commitment to advancing cybersecurity in the maritime domain.

Additionally, during the Singapore Maritime Week (SMW) 2025, one of our researchers had the opportunity to meet a representative from CyWhale on the sidelines of SMRC 2025. The discussion sparked interest in using our MariOT platform to evaluate CyWhale's cybersecurity products in a controlled, shipboard OT environment, marking a promising step toward future collaboration.

Finally, iTrust thanks the SMRC 2025 organizers, especially from Singapore Maritime Institute (SMI) for hosting such a dynamic inaugural event and looks forward to future opportunities to share our work and collaborate with the broader research community and industrial partners.

FIGURE Event

## Forum for Industry, Government and University Research knowledge Exchange (FIGURE)

iTrust was invited by Ofgem (the Office of Gas and Electricity Markets), a regulator for the electricity and downstream natural gas markets in Great Britain, to speak at its biannual FIGURE event on 10 Jun. FIGURE's objective is to build a research community for the Energy sector in the UK for sharing knowledge, expertise and experience. One of the focus in the Forum was to identify how applied research can help organisations in the energy sector increase cyber resilience through innovation. iTrust's Cyber Tech Lead, Siddhant Shrivastava, delivered a talk on iTrust's experience and lessons distilled from having organised and supported various international and national cyber exercises for the past decade. Titled "The RGB (Red, Green, Blue) of Cyber Exercise,"


*Fig 1.: Mark, iTrust's Assistant Director, and Siddhant, iTrust's Cyber Tech Lead, introducing our testbeds to the attendees of FIGURE via zoom. [Photo credit: Ofgem]*

Siddhant highlighted key learning points from CISS (Red), Locked Shields (Green) and CIDeX (Blue) cyber exercises, and how universities can play an active role in leading transformative cybersecurity initiatives to benefit countries in increasing their cyber posture, especially in critical infrastructure resilience.

LS 2025

## Locked Shields 2025 – iTrust's Continued Contribution to Global Cyber Defence

*By: Siddhant Shrivastava, Cyber Tech Lead, and Aanand R, Cyber Security Technology Engineer, iTrust*

Locked Shields 2025 (LS25) marked the 15th anniversary of the world's largest and most technically advanced live-fire cyber defence exercise. Organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), LS25 brought together more than 4,000 cyber defenders from 40 nations, simulating large-scale cyber-attacks on critical military and civilian infrastructure in a highly realistic, time-compressed environment.

Held in Tallinn, Estonia, LS25 consisted of two phases:

- Partners Run (01–03 April 2025): A preparatory event enabling participating nations to review scenarios, validate infrastructure, and conduct walkthroughs.
- Main Execution (04–09 May 2025): The core live-fire phase involving real-time cyber operations against simulated national systems.

iTrust is proud to support CCDCOE in Locked Shields for the fifth year running. Along with the Digital and Intelligence Service, iTrust served as Singapore's Green Team (GT) to support the cyber exercise. Together, they were responsible for the design, deployment, and maintenance of the digital version of the Secure Water Treatment (SWaT) system—an operational technology (OT) testbed presenting advanced ICS challenges to participating Blue Teams (BT). ITrust and DIS also worked closely with Mr. Bernhard Lippe, the CCDCOE GT Lead, as well as Mr. Daniel Guthy, the Special Systems Sub-Team Lead, to ensure the system was successfully deployed and executed during both the Partners Run (full-dress rehearsal) and Main Execution (actual exercise).


*Fig2.: (Left to right) Aanand and Siddhant with representatives from iTrust's sister lab, the National Cybersecurity R&D Laboratory (NCL), Wei Wei and Niklaus Kang*

LS25 proved to be significantly more demanding than previous editions, both technically and operationally. The GT overcame complex debugging challenges, managed heavy operational loads, and maintained effective team coordination across time zones and national boundaries. At the conclusion of the exercise, CCDCOE issued a letter of commendation to iTrust in recognition of its contributions to the overall success of LS25.

Collaboration

## iTrust -TalTech Collaboration

On April 16th, 2024, TalTech Estonian Maritime Academy signed a Memorandum of Understanding with the Maritime and Port Authority of Singapore (MPA), Singapore Maritime Institute (SMI), Singapore University of Technology and Design (SUTD) and Estonian Foundation CR14 to collaborate on maritime cybersecurity research and development activities.

The MoU facilitated collaboration through the mobility of experts and conducting applied research and training using the MariOT (Maritime Testbed of Shipboard Operational Technology) system to engage

the community and provide value in collaboration with the industry.


***Fig3.: Siddhant (left), iTrust's Cyber Tech Lead, and Aanand (right), iTrust's Cyber Security Technology Engineer, at their visit to TalTech***

Following more than six months of close collaboration between the MoU partners on joint maritime cybersecurity efforts, the MariOT system was successfully inaugurated on Thursday, March 20th.

A delegation from TalTech visited Singapore for two weeks to advance the collaboration. During their visit to iTrust, they met with the team of experts dedicated to MariOT, who presented their completed work and discussed future collaborative activities.

More information about the MoU signing can be found here.

## Reciprocal Visit to Estonia

As part of the ongoing collaboration, iTrust's Cyber Tech Lead Siddhant and Cyber Technology Engineer Aanand made two strategic visits to the Estonian Maritime Academy in March and May. During these visits, they worked closely with TalTech partners to finalise comprehensive plans for future maritime cybersecurity training programs. The collaborative planning sessions resulted in a framework that will support both online and in-person training modalities, ensuring flexible access to maritime cybersecurity education for participants across different geographical locations. These visits strengthened the partnership and established concrete pathways for knowledge transfer and capacity building in maritime cybersecurity.

NSF Trip

## National Science Foundation (US) Collaboration Trip organised by CSA

*By: Assoc Prof Daisuke Mashima, SUTD*

Assoc Prof Daisuke Mashima, along with the CyberSG Research & Development Programme Office (CRPO), Nanyang Technological University (NTU), and Singapore Management University (SMU), was part of a delegation led by the Cyber Security Agency of Singapore (CSA)to the US in March 2025. The trip was part of CSA's ongoing efforts to reinforce collaboration with National Science Foundation (NSF) in the US for cybersecurity R&D. CSA and NSF arranged the fruitful agenda throughout the stay, and we visited multiple reputable universities.

***Fig4.: Visit to the National Science Foundation (NSF)***

The first visit was a discussion with Prof Farshad Khorrami at NYU, who shared their research on autonomous system and OT security, including smart power grid systems. Many of them have close relevance to the scope of iTrust, and there is a great potential for collaboration in these areas. NYU's co-generation plant testbed is complementary to iTrust's EPIC testbed to enhance the coverage of the research in smart grid security. There was also keen interest from the team in the newly-developed maritime OT testbed (MariOT) in iTrust for experimenting attacks and defence tactics in the maritime domain.

At WINLAB in Rutgers, we had a tour of their globally-recognized wireless communication testbed. The discussion with Prof Aggelos Bletsas indicated potential collaboration opportunity in applying and evaluating


*Fig5.: Visit to New York University (NYU)*

their sensing technologies based on communication theory for monitoring as well as detecting attacks in iTrust testbeds.

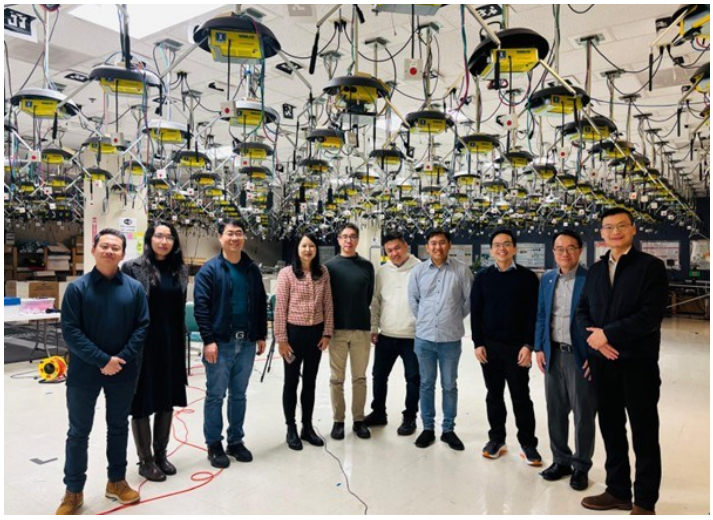

*Fig6.: Visit to WINLAB at Rutgers*

Prof Walid Saad and Prof Ryan Gerdes at Virginia Tech have been actively working on CPS security, including smart grid and autonomous control systems. Prof Gerdes was interested in physical-layer attacks and defenses as well as cyber-physical, cross-layer defence technologies, which are well aligned with iTrust's research strength, and thus it is promising to explore shared interest for the joint research.

During the whole-day visit at CyLab of Carnegie Mellon University, we learned research activities in ICS/OT security led by Profs Lujo Bauer, Pingbo Tang, and Eunsuk Kang. In particular, I was very glad to know Prof. Kang has been conducting research using iTrust's SWaT testbed and appreciated the value of the testbed. Besides the research discussion, Prof Hana Hibshi and Ms Megan Kerns introduced picoCTF, a well-established CTF event, with which iTrust's CISS could potentially join forces.


*Fig7.: Visit to Virginia Tech*

Last but not the least, our last stop was University of Pittsburgh, where we had a fruitful information sharing session with faculty members of the Laboratory of Education and Research on Security Assured Information Systems (LERSAIS). LERSAIS, led by Prof James Joshi, has strong connections in UPMC, one of the largest healthcare providers in the US and thus very active in cybersecurity and privacy research in the medical and healthcare domains. Prof Mai Abdelhakim is working on IoT and cyber-physical systems security. He and I had a follow-up call, which resulted in collaboration to organise IEEE Workshop on Security and Resiliency of Critical Infrastructure and Space Technologies (IEEE SR-CIST 2025).


*Fig8.: Visit to CyLab at Carnegie Mellon University*

Thanks to the invaluable leaderships by CSA and NSF, it is envisioned that the Singapore-US collaboration will be significantly reinforced in the coming years. I hope these introductory meetings will lead to joint research projects that can make our societies secure and trustworthy.

Featured on Media

## Article Summary: iTrust featured in CNA episode for Device Repair Investigation

Media Coverage by **Channel News Asia** | Click **here** to watch on Youtube |

Background: Channel News Asia's "Talking Point" documentary series conducted an investigation where 40 devices were sent to repair shops, revealing that 12 devices (3 phones, 9 laptops) had been snooped on by technicians. The investigation used screen recording software developed by NUS Greyhats to catch technicians accessing personal files, photos, and accounts. Expert Analysis and Risk Assessment: Siddhant Shrivastava, Cyber Tech Lead at SUTD's iTrust Centre for Research in Cyber Security, served as the cybersecurity expert providing analysis on the potential harms from data breaches during device repairs. Demonstration of Advanced Threats: Using Talking Point producer Dynn Othman's damaged MacBook as a case study, Siddhant demonstrated sophisticated attack scenarios that malicious technicians could execute:

*Fig9.: Siddhant Shrivastava, iTrust's Cyber Tech Lead, dives into the depths of a snooper's mind for Talking Point. (Photo credit: Channel News Asia)*

AI Voice Cloning: He showed how a technician could access WhatsApp and Telegram accounts linked to the laptop and use AI tools to clone the owner's voice within just two minutes Social Engineering Attacks: Created a realistic AI-generated audio message mimicking Dynn's voice asking contacts for money, demonstrating how scammers could exploit personal data for financial fraud Stealth Operations: Explained how sophisticated attackers could time their scams when the real device owner isn't available to maximize success

Key Expert Insights: Siddhant emphasised that the tools required for such attacks are "designed for the layperson" and that "one doesn't have to be a super hacker," highlighting how accessible these attack methods have become. He categorized the threat spectrum from casual snooping by "bored technicians" to serious criminal activities including blackmail using large amounts of personal data. iTrust's Contribution: The centre's involvement demonstrated the real-world cybersecurity risks that everyday consumers face, providing technical expertise to illustrate how seemingly minor privacy breaches during device repairs can escalate into sophisticated social engineering attacks using readily available AI technology.

## Article Summary: Smart Home Device Security Investigation

Media Coverage by **Channel News Asia** | Click **here** to watch on Youtube |

Background: Channel News Asia's "Talking Point" conducted an investigation into the vulnerability of smart home devices with cameras, revealing how easily these devices can be hacked and compromised.

Demonstration of Network Infiltration: Siddhant Shrivastava, from iTrust Centre for Research in Cyber Security at SUTD, served as the cybersecurity expert demonstrating advanced attack scenarios once hackers gain initial access to smart home networks. With 8 years of experience studying how smart devices can be exploited, Siddhant provided critical technical

*Fig10.: Siddhant Shrivastava, iTrust's Cyber Tech Lead, featured on Talking Point 2024/2025 - Are You Being Watched? (Photo credit: Channel News Asia)*

expertise for the investigation. Simulated Smart Home Environment: Siddhant, with the help of iTrust Research Fellow Dr Yan Lin Aung, created a realistic test environment replicating a typical home Wi-Fi network where multiple smart devices from various brands connect to a single router and are controlled through one master app. This setup included smart plugs controlling everyday appliances like lights, chargers, toasters, fridges, and fans.

Chain Reaction Attack Demonstration: Using a compromised smart camera as the entry point, Siddhant demonstrated how hackers can:

Network Reconnaissance: Use the camera's operating system to ping and identify all other devices on the home network

Lateral Movement: Exploit the camera as a "command and control center" to access other smart devices

Complete Network Compromise: Show how a single vulnerable device can lead to control over the entire smart home ecosystem

Key Technical Insights: Siddhant explained how attackers can write simple scripts to remotely control all connected devices, even while homeowners are sleeping. He emphasized that what appears to be a minor weakness in one device can trigger a "major chain reaction across the entire network."

He illustrated how the Wi-Fi router serves as the central point in a home's cyber ecosystem, and how a compromised device like a CCTV camera can intercept sensitive information such as passwords, bank statements, and other personal data transmitted through the network.

iTrust's Contribution: The centre's involvement provided viewers with a comprehensive understanding of the cascading security risks in interconnected smart home environments, demonstrating real-world attack scenarios that go beyond simple device hacking to complete network compromise.

## Internship

iTrust is dedicated to upskilling individuals and organisations through a diverse range of programmes: hands-on training, workshops, and internships. We offer comprehensive programmes that are designed to create awareness, enhance knowledge and skills, and foster innovation in the ever-evolving landscape of cyber security.

As part of our mission to be Singapore's one-stop centre for research, training, and education, we regularly receive students from various background as interns. Here are some of their stories in their internship joruney.

## Reflections

Meet our four talented interns from Catholic High School: Cheng Yang, Fung Yik Yu Myron, Tang Zhimo, and Le Khanh Hung. Under the guidance of **Andy Tay**, iTrust's Education Lead, they've explored real-world applications of cybersecurity and demonstrated their creativity through a series of informative infographics.

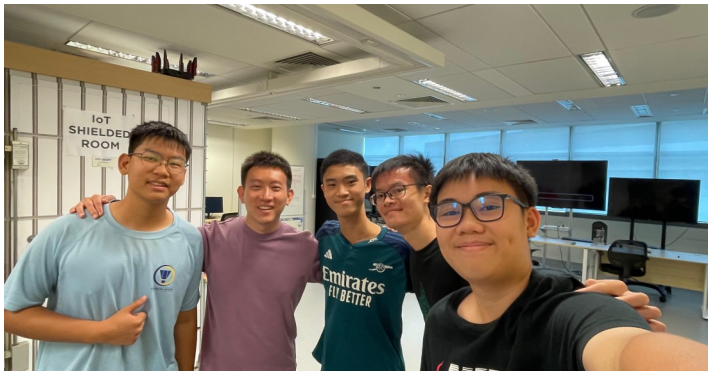


*Fig11.: Catholic High School Interns pictured with Andy Tay, iTrust's Education Lead (from left to right: Tang Zhimo, Andy Tay, Cheng Yang, Fung Yik Yu Myron, and Le Khanh Hung)*

Scan the QR code to view the infographics they created and see what they've been working on!


*By: Cheng Yang, Student at Catholic High School*

From 26 May to 13 June 2025, I had the privilege of interning at iTrust. When I first began the internship, I had very limited knowledge about cybersecurity or Operational Technology (OT). However, what started as unfamiliar territory quickly became a field of deep interest, as my learning over the three weeks was truly exponential. Each new concept built on the last, and with every day, I gained not only knowledge but also confidence in navigating complex systems.

One of the most impactful aspects of the internship was the guided tours of the testbeds—SWaT (Secure Water Treatment), EPIC (Electric Power and Intelligent Control), WaDI (Water Distribution), and the IoT testbed. These visits allowed me to see firsthand how OT systems operate in real-world environments. They also helped me understand the critical role cybersecurity plays in protecting infrastructure that societies depend on every day.

After the tours, we transitioned into self-directed learning, where I explored OT architecture, core terminologies, and how networks are both essential to and vulnerable within these systems. This approach helped me develop a macroscopic understanding of how different components interact, and how each layer of the system must be secured.

One of the highlights of my internship was the opportunity to create Capture the Flag (CTF) questions focused on industrial communication protocols like DNP3. Designing these challenges pushed me to think more deeply about how these systems work, and how attackers might attempt to exploit them. It also allowed me to contribute something meaningful while sharpening both my technical, creativity and problem-solving skills. None of this would have been possible without the consistent support of our mentor, Mr Andy Tay. He regularly checked in, guided our research and learning throughout this internship. His mentorship was instrumental in transforming what could have been a surface-level introduction into an experience of exponential learning and personal growth.

This internship has given me a solid foundation in cybersecurity and OT systems, but more importantly, it has sparked a genuine curiosity and passion for this field. I am deeply grateful for this opportunity, and I would wholeheartedly recommend an internship at iTrust to any student interested in technology, cybersecurity, or the systems that keep our world running. It is an eye-opening and enriching experience that goes far beyond the classroom.

*By: Fung Yik Yu Myron, Student at Catholic High School*

My experience at the iTrust internship was a very fruitful and insightful one. Firstly, we were introduced to the different testbeds in iTrust, such as the Secure Water Treatment (SWaT) and the Internet of Things (IoT) testbeds. These guided tours offered critical insight about the driving forces behind the different aspects of our lives, such as utilities and power. We then learnt about different aspects of operational technology (OT) and expanded our knowledge on technology and cybersecurity. Next, we consolidated our knowledge by creating an infographic on OT. This helped us solidify our understanding about OT, which would be important in learning the subsequent information later on.

Next, we learned more about cybersecurity through the creation of capture the flag (CTF) questions. Initially, we had no idea or experience on cybersecurity but through the guidance and mentorship of our supervisors, we were able to create our own CTF questions. This process allowed us to exercise creativity and critical thinking as we needed to craft questions that AI chatbots, such as ChatGPT, could not solve. We created CTF questions on various topics such as ciphers and communication protocols. These were aspects used in encryption and communication between different systems in the real world.

One of my highlights in this internship was learning to hack the SWaT system. We applied knowledge gained from our self-directed learning about OT and cybersecurity and were given the opportunity to do hands-on work. This was a highlight because we were able to see real-time results of our coding which was very insightful to me. We also learnt the importance of cybersecurity measures such as firewalls and reset systems.

We would like to thank our mentor Mr Andy Tay, for his consistent guidance and support through this internship. He gave us valuable insights and advice about how to elevate our work, such as offering a different perspective on our CTF questions. We would also like to thank Mr Andrew Tay and Mr Aanand R for

guiding us through the hacking process and giving us the chance to use the testbeds.

Through this internship, I learnt more about OT and cybersecurity and also exercised my creativity and critical thinking. It was a very eye-opening and insightful experience. It has given me a foundation in the technological field and sparked my interest and passion in learning more about these fields. I am very grateful for this opportunity to take part in this internship and would recommend this to other students interested in the technological field.

*By: Tang Zhimo, Student at Catholic High School*

Over the past three weeks at iTrust, I had the incredible opportunity to work on the EPIC (Electric Power and Intelligent Control) testbed as part of my internship. This experience has been both engaging and rewarding, providing me with hands-on exposure to the world of cyber-physical systems and Operational Technology (OT).

During the internship, my teammate (Khanh Heng) and I made five Capture-the-Flag (CTF) challenges related to EPIC. These challenges tested our problem-solving skills and deepened our understanding of OT security. To consolidate our learning and share our insights, we also created an infographic that presents EPIC's structure, purpose, and key vulnerabilities in a clear and visual format.

One of the most exciting parts of the internship was conducting two simulated cyber-attacks on the EPIC system. The first was a Variable Speed Drive (VSD) attack, and the second involved attacking the load of the EPIC infrastructure to simulate attack to the housing. Through these exercises, I learned not only about how cyberattacks are executed but also about the importance of securing critical infrastructure.

Throughout the journey, we were guided and supported by Andrew and Andy, who were incredibly friendly, patient, and knowledgeable. Their mentorship made the learning environment welcoming and productive, and I'm truly grateful for their support.

Overall, this internship has sparked a deeper interest in OT cybersecurity and has given me practical experience that goes far beyond the classroom. I'm very thankful for the opportunity to be part of the iTrust community, and I would definitely recommend this experience to anyone curious about OT, cybersecurity, or critical infrastructure systems.

*By: Le Khanh Hung, Student at Catholic High School*

During my internship at iTrust, I had the valuable opportunity to explore and learn about various test beds such as SWaT, EPIC, WADI, MariOT, and the IoT test bed. These guided tours, conducted by the engineers at iTrust, deepened my understanding of the critical role these test beds play in simulating and securing cyber-physical systems like water treatment plants and power grids. I gained a clearer perspective on the importance of cybersecurity in protecting these essential infrastructures.

Following the tours, my partner and I worked on designing Capture-The-Flag (CTF) challenges related to encryption and communication protocols used in the EPIC test bed. With guidance and feedback from our supervisor, Mr Tay, we refined our questions to ensure they accurately reflected the systems and challenges within EPIC. This process helped us develop a stronger sense of realism and relevance in our tasks.

We also had the chance to come up with two cyberattacks on the EPIC test bed. The first involved manipulating the Variable Speed Drives (VSDs) to trip the power supply from the motor-generator set, and the second simulated a household power outage by overloading the electrical load. Mr Andrew, one of the engineers, provided us with reference code that greatly supported the development of these attacks, while still allowing us the space to apply our own problem-solving skills.

Throughout this internship, both Mr Tay and Mr Andrew were approachable, supportive, and encouraging. Their balance of guidance and autonomy enabled us to grow in confidence and technical capability. Overall, my experience at iTrust was highly meaningful and insightful, enriching both my understanding of cybersecurity in critical systems and my appreciation for collaborative engineering work.

## General Enquiries

iTrust: *itrust*

NSoE: *nsoe_destsci*

CiMS: *cims*

*Email addresses end with the domain* ***@sutd.edu.sg***

**Scan to view previous issues of iTrust Times**

## Management

**Prof. Jianying ZHOU**

Centre Director, iTrust, Singapore University of Technology and Design

Professor, Information Systems Technology and Design (ISTD), Singapore University of Technology and Design

*jianying_zhou*

**Prof. Aditya P MATHUR**

Founding Centre Director, iTrust, Singapore University of Technology and Design

Director, National Satellite of Excellence, DeST-SCI Professor Emeritus, Computer Science, Purdue University

*aditya_mathur*

**Mark GOH**

Assistant Director, iTrust

*mark_goh*

## iTrust Laboratories

**Shrivastava Siddhant**

Cyber Tech Lead

*shrivastava_siddhant*

**Andy TAY**

Education Lead

*Andy_tay*

**Aanand R**

Cyber Security Technology Engineer

*Aanand_r*

**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*