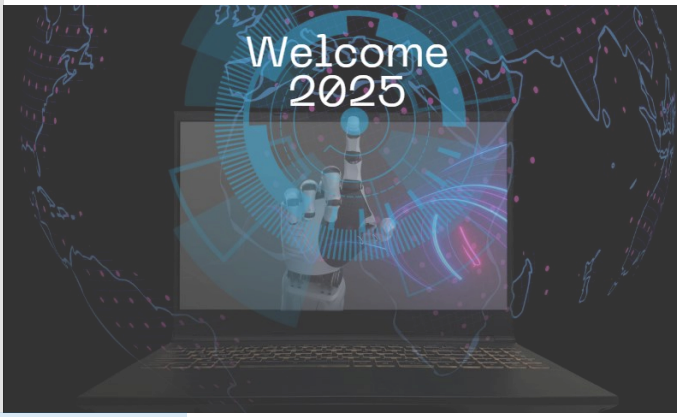
iTrust Times

A Quarterly Newsletter

Issue Highlights:



Oct—Dec 2024 | Volume 10 Issue 4

From Centre Director's Desk

Dear readers,

Happy New Year to friends of iTrust!

iTrust has been working closely with industry partners. An MoU was signed among ST Engineering Info-Security, SUTD and Wärtsilä ANCS, to cooperate in vulnerability discovery and validation, engineering and solution, and cyber drill in the maritime sector. iTrust also awarded Ensign InfoSecurity a contract to translate iTrust's anomaly detection technologies for deployment in water and wastewater treatment plants. These efforts, supported by our key partners in CSA, MPA and SMI will significantly bolster Singapore's critical infrastructure security posture.

iTrust is also expanding its academia collaboration. At the international level, we hosted visitors Cardiff University and also visited a several cybersecurity research groups in Germany and Hungary, including Munich University of Applied Sciences, Passau University, Karlsruhe Institute of Technology, and Budapest University of Technology and Economics. The common research interest is in OT cybersecurity. iTrust has also offered internship opportunities to high school students, undergraduates and postgraduates to study and conduct experiments at iTrust's world-class OT testbeds.

iTrust has been very active in cyber exercises by leveraging our unique OT testbeds. We supported MINDEF in organising the national cyber exercise CIDeX in Nov 2024, to train critical infrastructure operators in identifying and responding to cyber attacks. Among the six OT systems used in CIDeX 2024, three were contributed by iTrust. iTrust was involved in the annual Deutschlands Bester Hacker (DBH) in Sep 2024 as well. iTrust is currently planning to contribute to the NATO's Locked Shields exercise 2025, billed as the world's largest live-fire cyber defence exercise.

2025 will yet be another busy year for iTrust. The new maritime shipboard OT testbed MariOT will be commissioned in Mar 2025. This will be a new milestone for iTrust to explore maritime cybersecurity R&D, professional training and cyber exercise. We will also develop an R&D master plan for iTrust for the next five years. We look forward to closer collaboration with partners from academia, industry and government agencies in the coming year, in efforts for securing the critical infrastructure.

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

CSA SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

MoU Signing

SUTD-STE- ANCS MoU

On 17 Oct 24, a memorandum of understanding (MoU) was signed among SUTD, ST Engineering Info-Security, and Wärtsilä ANCS. Under the MoU, the parties will cooperate in vulnerability discovery and validation, engineering and solution, and tabletop exercise and cyber drill in the maritime sector.

Fig 1.: Prof Jianying Zhou, Centre Director (third from left) in the MoU Signing on 17 October, with (from left to right) Prof Tony Quek, Pillar Head, ISTD Pillar, SUTD, Mr Marko Lim, General Manager, ANCS Customer Delivery Asia, Mr Mark Latusseck, Managing Director, ANCS Germany, Mr Lim Meng Hwee, Senior Vice President / Head at ST Engineering, Cyber Solutions & Infrastructure Group, Mr Goh Eng Choon, President, Cyber, ST Engineering Info-Security Pte Ltd.

Translation Contract

Award to Ensign

In Dec 24, iTrust awarded Ensign InfoSecurity Pte Ltd a contract to translate iTrust's anomaly detection technologies for deployment in water and wastewater treatment Plants.

These technologies, Distributed Anomaly Detection (DAD) and AICrit, developed in-house by iTrust, are engineered to ensure the secure and reliable operation of industrial control systems. These innovations enhance anomaly detection and response capabilities, reinforcing the resilience and operational integrity of critical infrastructures. The data fusion platform will encompass the capability of supporting several pipelines for data ingestion, development, deployment, and maintenance of iTrust technologies. As a pivotal step towards translating research into practical applications, the platform will rigorously evaluate DAD and AICrit against established industrial standards. This initiative, funded by the Cyber Security Agency of Singapore under the National Cybersecurity R&D Programme, will significantly bolster Singapore's critical infrastructure security posture.

This strategic partnership will see Ensign InfoSecurity working closely with iTrust researchers to develop and deploy a state-of-the-art data fusion platform. The platform is designed to evaluate locally developed anomaly detection technologies, with a primary focus on bridging research-to-market gaps and addressing deployment challenges. This collaboration also underscores iTrust's commitment to advancing cybersecurity solutions and fostering the adoption of cutting-edge technologies in critical infrastructure.

Conferences

GovWare

As part of the Singapore International Cyber Week, iTrust participated in GovWare 2024 as an exhibitor. Held from 15 to 17 Oct 24 at the Sands Expo and Convention Centre, GovWare brought together more than 13,000 national and international cyber experts, academics, leaders and policy makers to exchange knowledge on key cyber security issues and solutions. During the exhibition, iTrust showcased the research work from the second phase of the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure (NSoE -DeST-SCI) as well as the CSA-iTrust Master of Science in Security by Design Scholarship (CiMS) programme.

Fig 2.: Siddhant, iTrust Cyber Tech Lead, introducing iTrust's projects and CiMS programme to government officials from China.

Defense TechConnect Innovation Summit

In Aug 24, iTrust was invited to submit innovative technologies to be pitched and showcased at the Defense TechConnect Innovation Summit. Established in

2012, the Summit is the United States' largest innovation matchmaking programme and allows the nation's Department of Defense (DOD) to address national security priority challenges by identifying, adopting and deploying new technologies and processes. It does this by connecting early-stage technologies with the DOD for federal funding opportunities, while emphasising dual-use innovations that can benefit civilian and government sectors.

iTrust Founding Centre Prof Aditya Mathur and Assistant Director Mark Goh co-wrote a submission

Fig 3.: Mark (left) and Aditya at their Defense TechConnect booth showcasing iTrust's cyber twins

"Cyber Twins for Professional Training, Cyber Drills and R&D." Traditionally, digital twins have been categorised as component / asset / system / unit, and process twins. iTrust has developed a fifth category, termed cyber twin. Our in-house developed cyber twins are rapidly configurable within a domain (e.g., different water utilities) and across different domains (e.g., gas pipelines and electric power grids.) Because our cyber twins allow users to understand and appreciate the effects of cyber-attacks: (1) visually, in a safe and realistic environment; (2) without the need to disrupt real plant operations; and (3) without the need to invest in building realistic physical testbeds, they can be used for education, professional training, cyber drills and R&D.

Our submission was accepted by the committee for pitching and showcasing, and Aditya and Mark were in Austin to set up a booth and made a pitch to potential investors from 3 to 5 Dec 2024. We met with like-minded early stage innovators from universities and private sector, small business associations and consultants who could assist start-ups with the entire fundraising and project lifecycle, and government and private funders. As a follow-up, Prof Aditya will be meeting with one of the venture capitalists in Atlanta to

Fig 4.: Aditya (standing) presenting the cyber twins to participants and technology panel and investors (seated, front row)

deep-dive into iTrust's GURU platform, for which she had shown interest in using for education.

GURU (Guided Universal Resource for Understanding) is an integrated platform for instructors to deliver an engaging active learning experience for students in an in-person lab environment or via a remote online classroom. A subset of GURU, called GURU CPS, is applied in the field of Operational Technology (OT) Cyber-Physical systems (CPS) with specific OT tools (such as a digital twin of a water treatment plant). GURU CPS is based on the digital twin of iTrust's Secure Water Treatment (SWaT) plant.

TechInnovation 2024

By: Sanat Khandekar, Research Assistant

TechInnovation is Asia's premier technology-matching platform which aims to connect various stakeholders within the global tech industry with innovators to encourage the discovery of new technology and explore potential avenues for commercialisation of cutting-edge research.

As part of the team representing iTrust, I prepared informative material and the technical background for

Fig 5.: Sanat (left), iTrust Research Assistant, explaining the IT-OT Bridge concept to Mr Karthikk Subramanian, Senior Staff Engineer from Panasonic R&D Center, Singapore.

my project: "IT-OT Bridge: AI-Based Early Intrusion Detection for Industrial Control Systems". Over the three days, our booth was approached by a handful of industry professionals and potential collaborators. The questions ranged from technical to business related. My efforts in marketing the technology was in line with iTrust's goal to seek more collaborators and licensors.

Fig 6.: Lim Qinxin (left), SUTD Undergraduate student, Sanat Khandekar representing iTrust at TechInnovation 2024.

Academic Visits

Exploring Collaborations in IT and OT Cybersecurity: iTrust and NCL Academic Visits to German and Hungarian Universities

By: Siddhant Shrivastava, Cyber Tech Lead, iTrust and Liu Yuancheng, Head of Technology, NCL

From 26 Sep to 2 Oct 24, a team from sister labs iTrust and the National Cybersecurity R&D Laboratory (NCL) visited several prestigious universities and research institutes across Germany and Hungary to explore IT and OT cyber security collaborations. The trip also helps to showcase and raise awareness of Singapore's cyber security capabilities to an international audience.

Munich University of Applied Sciences

On 26 Sep we met with Prof Thomas Schreck and Prof Michael Heinl, whose applied research focuses on OT systems cybersecurity, hardware security, and digital identities. We discussed potential collaborations, particularly around integrating NCL's railway IT-OT

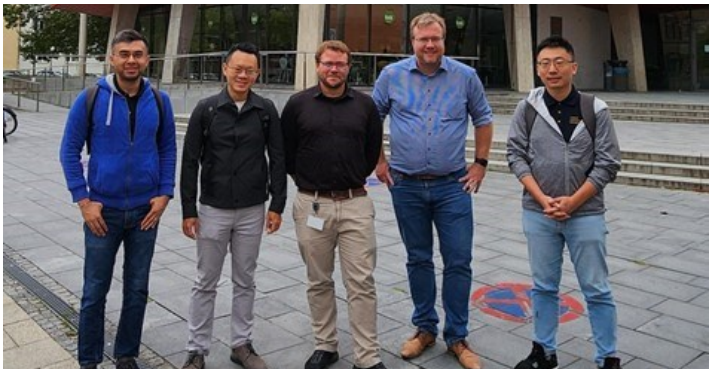


Fig 7.: (Left to right) Siddhant Shrivastava, Mark Goh, Prof Michael Heinl, Prof Thomas Schreck, Yuancheng Liu at the Munich University of Applied Sciences

cyber range and power grid digital equivalent system into their courses. Both the professors expressed an interest in using iTrust Cyber Twins for their upcoming courses in cyber-physical systems. Some key points included exploring license models, local deployment options, and academic partnerships for research publications. As a follow-up from the visit, iTrust is now in advanced discussions with Prof Heinl to use the iTrust Cyber Twins for his classes in Mar 2025.

Passau Institute of Digital Security, Passau University

Fig 8.: Control system rig for exploring cyber attacks on autonomous vehicles

On 27 Sep, we were hosted by Prof Joachim Posegga and Prof Stefan Katzenbeisser in Passau University. Their lab has been active in researching the security of EVs and the German railway system. We went away extremely impressed by their team's deep expertise and extensive work in securing railway systems, and they have agreed to provide research questions towards iTrust and NCL's plans in the cyber protection of Singapore's transportation system. To that end, Prof Katzenbeisser helpfully shared two papers on securing the railway systems that he co-authored.

Fig 9.: CEO of DBH, Timo Stark, going through step-by-step solutions of the challenges contributed by iTrust and NCL

Deutschlands Bester Hacker, Dortmund

Back in May, we were introduced by the Digital Intelligence Service to Mr Peter Wilfhart, Chief Digital Officer of the Oberfranken Bayreuth Chamber of Commerce, who was keen to tap into iTrust and NCL's cyber capabilities in providing CTF challenges to the annual Deutschlands Bester Hacker (DBH) that his team organises. Having contributed to four challenges, we were invited to attend the DBH Finals on 28 Sep in Dortmund to provide the technical debriefs on our submitted challenge statements to the participants. The exercise followed a CTF format that required the participants to understand OT systems and protocols such as MODBUS. Over 2.5 hours, 35 hackers tried to solve the timed challenges. As not all were familiar with OT protocols, they came up with creative ways, including the use of AI, to understand and solve the challenges. DBH also provided CTF challenges to iTrust's annual Critical Infrastructure Security Showdown cyber exercise, showcasing the close international cooperation among the three parties.

Fig 10.: (Left to right) Siddhant Shrivastava, a CTF participant, Mark Goh, Peter Wilfhart, Yuancheng Liu, Timo Stark at the evening reception following the DBH finals

Karlsruhe Institute of Technology, Blankenloch

Fig 11.: The various testing facilities and laboratories at KIT, with Dr Ghada Elbez (top right) providing an overview of her group's research

On On 30 Sep, we had a half-day visit to the Karlsruhe Institute of Technology at its Blankenloch campus. The visit started with a lunch with the heads of the institute followed by a general introduction about the OT security research conducted by iTrust and NCL. Dr Ghada Elbez, who is the head of the Secure Energy Systems (SES) group, introduced us to their work in the protection and resilience of energy systems. Following a tour of their extensive testing facilities and laboratories - real-time distribution systems and simulators - with her researchers and PhD students, we had deep-dive discussions on power grid operation scenarios and attack datasets, and how NCL's expertise can support their research platform. Mark also expressed the possibility of connecting the testbeds and federating cyber ranges among iTrust, NCL, and KIT.

EIT Digital, Budapest

Fig 12.: (Left to right): Krisztián Gál, Yuancheng Liu, Siddhant Shrivastava, Gergely Horváth at EIT Digital

On 1 Oct, we visited EIT Digital in Budapest to present the comprehensive IT/OT/IoT workshop that NCL currently offers for cybersecurity training. During our

visit, EIT ecosystem lead Krisztián Gál elaborated on EIT Digital's mission to drive digital technology innovation. We explored potential collaborations on professional OT cybersecurity training, certification programs, and the possibility of utilising NCL's and iTrust's advanced cyber range capabilities for educational and industrial workshops as well as potential commercialisation opportunities for iTrust's patented technologies in the European market.

Eötvös Loránd University (ELTE), Budapest

Fig 13.: Yuancheng Liu (far left, standing) and Siddhant Shrivastava (second from right, standing) with their hosts from ELTE

Later in the afternoon, we met with Prof Tamás Holczer, Prof Imre Lendak, and their research group, focusing on water system security and honeypot technologies. The meeting began with Prof. Tamás Kozsik, the dean of the university, introducing the different research activities and potential collaboration avenues. We explored student exchange programs and collaborative research projects, especially in the railway security domain. The PhD students expressed a deep appreciation for iTrust's SWaT datasets that they have been using in their research.

CrySyS Lab, Budapest University of Technology and Economics

During our visit to the CrySyS Lab on 2 Oct, we met with Prof. Gergely Biczók, where we discussed their work on security and privacy of machine learning systems as well as some work in different critical infrastructure sectors. We also considered potential cooperation between GPU services and PLC honeypot technologies, a crucial area for advancing OT system security. Siddhant agreed with the professors that the iTrust Cyber Twins can be useful in their applied Masters programme in cybersecurity which has a component focusing on cyber-physical systems.

Awards

iTrust Team Wins Best Paper Award at ATIS 2024

A research team from iTrust, led by Research Fellow Dr Gauthama Raman, has won the Best Paper Award at the International Conference on Applications and Techniques in Information Security (ATIS) in Nov 24. This recognition highlights the team's excellent work in addressing critical challenges in water utility management using advanced machine learning techniques. The paper, titled "Adaptive Data-Driven LSTM Model for Sensor Drift Detection in Water Utilities," is authored by S. Abisheg, a student intern at iTrust, Dr Raman, and Prof. Aditya P Mathur, the founding centre director of iTrust and director of the National Satellite of Excellence (NSoE).

Abstract: The paper introduces an adaptive Long Short -Term Memory (LSTM) model designed for detecting sensor drift in water treatment plants. Sensor drift, a common issue in critical infrastructure, can lead to inaccurate readings and operational inefficiencies if left unaddressed. The proposed model employs a data -driven approach to identify and predict sensor anomalies, enabling proactive maintenance strategies. This capability is crucial for ensuring the reliability and security of water utilities, a cornerstone of public health and safety.

Practical Impact: This research contributes towards the ongoing efforts in predictive maintenance for water treatment facilities. By accurately detecting sensor drift, the adaptive LSTM model empowers operators to mitigate risks, optimize resource utilization, and maintain high standards of service. The work's implications can extend beyond water utilities, offering a scalable framework for monitoring and securing sensors across various critical infrastructures.

Acknowledgments: This research was made possible through funding and support from the Cyber Security Agency of Singapore (CSA), under its National Satellite of Excellence Programme "Design Science and Technology for Secure Critical Infrastructure: Phase II" (Award No: NRFNCR25-NSOE05-0001). The team extends its gratitude to CSA for enabling the exploration of innovative solutions to real-world Challenges.

Visits & Seminar

Cardiff University - Visit and Seminar

iTrust hosted Dr Yulia Cherdantseva, Prof Yingli Wang and Dr Angharad Watson from Cardiff University on 11 Nov 24. Their visit was a follow up from iTrust Assistant Director Mark Goh's visit to Cardiff University a year earlier, where he was hosted by Prof Pete Burnap, Prof Omer Rama and Vojay Kumar. Dr Cherdantseva delivered an insightful seminar on "A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment." Dr Yulia presented a generic configurable dependency model of a SCADA system which captures complex dependencies within a system and facilitates goal-oriented risk assessment. This model was developed by collecting and analysing the understanding of the dependencies within a SCADA system from 36 domain experts.

Fig 14.: Dr Yulia presenting about SCADA systems to the attendees of her seminar.

Dr Yulia emphasised that the key purpose of SCADA system was to enable either an on-site or remote supervisory control and monitoring of physical processes of various natures, so in order for a SCADA system to operate safely and securely, a wide range of experts with diverse backgrounds must work in close rapport. Dr Yulia also presented the overall view of an entire system at a high level of abstraction which is accessible to all experts involved, this assists with gauging and assessing risks to the system. Since the SCADA system composed large numbers of interconnected technical and non-technical sub-elements, Dr Yulia endorsed the importance to capture the dependencies between these sub-elements for a comprehensive and rigorous risk assessment.

Following the seminar and a hosted lunch, Mark and the iTrust's cyber security technology engineers gave a tour of iTrust's testbeds. To seed discussions in collaborations, the Cardiff team also had a 5-min introduction to the research and outreach work by several iTrust researchers after the tour.

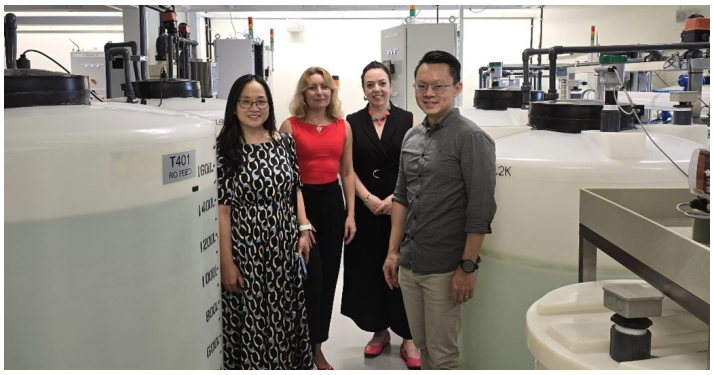


Fig 15.: Mark (far right), Assistant Director of iTrust, showing our guests from Cardiff University around in iTrust's labs. (from left to right: Prof Yingli Wang, Dr Yulia Cherdantseva, and Dr Angharad Watson)

Internship

Internship Reflections

By: Gui Shao Kai, Student, Catholic High School

iTrust welcomed three students from Catholic High School from 18 Nov 24 to 13 Dec 24 for a 4-week internship. During this period, they were each assigned a supervisor and were tasked to developed speech recognition for plant operation and development of OT systems and architecture academic structure. One of the students, Gui Shao Kai, summarised his internship as being "incredibly fruitful." He added:

"The internship began with an introduction to Operational Technology (OT) and critical systems. Through a physical guided tour of a miniature water treatment plant, we were acquainted with basic OT terminology and an overview of the inner workings of the system. This tour proved to be a pivotal point of my experience, providing a macro view of OT and making it much easier to connect the dots with the subsequent content we explored. Not only that, it demonstrated the importance of the critical systems sector, which served as a constant reminder of the value in learning about these systems.

Thereafter, the focus switched to self-directed learning, where we were tasked with understanding the specifics of OT systems. We had routine meetings in which we discussed our findings while Mr Tay gave us a direction to further research on. This approach to learning turned

out to be effective, giving us an opportunity to hone our critical thinking while allowing us to learn at our own pace. By the end of the internship, we had successfully grasped the fundamentals of OT.

I am grateful to have had this opportunity at iTrust. What I have learnt has far exceeded my expectations and ignited an interest in the OT sector. I would highly recommend an internship with iTrust to anyone considering it!"

Fig 16.: Andy Tay (far right), iTrust Education Lead, pictured with his three interns (from left to right) Gui Shao Kai, Brendan Tan, Jay Len.

At iTrust, we align our internship programs with the academic calendars of secondary and tertiary institutions. Term courses span across multiple terms while vacation courses are intensive learning programmes that are held during the first three weeks of school holidays. To apply an internship with iTrust, please write in to itrust@sutd.edu.sg.

iTrust Matters

General Enquiries

iTrust: *itrust*

NSoE: *nsoe_destsci*

CiMS: *cims*

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

Scan to view previous issues

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

Student Outreach Lead

Andy_tay

Aanand R

Cyber Security Technology Engineer

Aanand_r

Andrew TAY

Research Senior Technologist

andrew_taykongngee

National Satellite of Excellence

Jillian CHIN

Manager

jillian_chin

Angie NG

Manager

angie_ng

Siti Nadhirah Shaik NASAIR

Deputy Manager

siti_nadhirah

Vanessa LEE

Deputy Manager

vanessa_lee