iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jan—Mar 2025 | Volume 11 Issue 1

From Centre Director's Desk

Dear readers,

Greetings from iTrust!

2025 marks a new milestone of iTrust in the maritime sector. After two years of planning and sourcing for vendors to design and build the MariOT testbed, it was commissioned on 20 March 2025, in line for announcement during the Singapore Maritime Week a week later. MariOT is the fourth critical infrastructure testbed in iTrust, 10 years after the first testbed, SWaT, was launched. MariOT is funded by the Singapore Maritime Institute (SMI) and is a result of close collaboration with the Maritime and Port Authority of Singapore (MPA), ST Engineering, ANCS and ARI. MariOT is the world's first industrial grade cyber-physical testbed which has been certified by ClassNK in accordance with its Cyber Security Approach. MariOT is equipped with essential shipboard operational technology systems and offers a safe and realistic testing environment for cybersecurity technologies without disrupting actual vessel operations. Merging essential shipboard OT systems with virtual simulation models, the hybrid platform will be used to design and validate new cybersecurity technologies for deployment onboard ships. MariOT will enable in-depth research and training for academia, government agencies, and international collaborators through cyber exercises and drills, with the aim to strengthen cybersecurity resilience across the maritime sector.

2025 also marks an important milestone for iTrust in its push towards technology translation. Led by Prof. Aditya, iTrust is working closely with TWT, The Water Tower, which is a premier R&D center located in Buford, Georgia, USA, to pilot the cybersecurity technologies developed by iTrust. TWT has provided the dataset received from the water treatment plants, which is currently in use for creating models to demonstrate iTrust technologies for detecting anomalies in large physical plants.

iTrust has made a significant contribution to the cybersecurity community by sharing the datasets collected from iTrust's cyber-physical system testbeds. The invaluable datasets have been available to researchers across the world since 2016 and have been downloaded more than 18,000 times by researchers from 100 countries.

iTrust is also making waves in grooming the next generation of cybersecurity professionals by offering prestigious CiMS scholarship to MSSD students, as well as internship to local and international students.

To this end, I invite all interested parties to approach iTrust to explore ways we can join hands in R&D, training and education to help contribute towards a safer and more secure Singapore.

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

MariOT Updates

Commissioning of Maritime Operational Technology (MariOT) Shipboard Testbed

The commissioning ceremony of the new Maritime Operational Technology (MariOT) shipboard testbed was held in SUTD on 20 March 2025.

Fig 1.: Prof Phoon Kok Kwang, President of SUTD, delivering his welcome remarks.

Attended by more than 50 invited guests and media, the ceremony started off with SUTD's President, Prof Phoon Kok Kwang delivering the welcome remarks. This was followed by the commissioning of the testbed by Mr Lee Tzu Yang, SUTD's Chairman and Mr Teo Eng Dih, the Maritime and Port Authority of Singapore (MPA)'s Chief Executive.

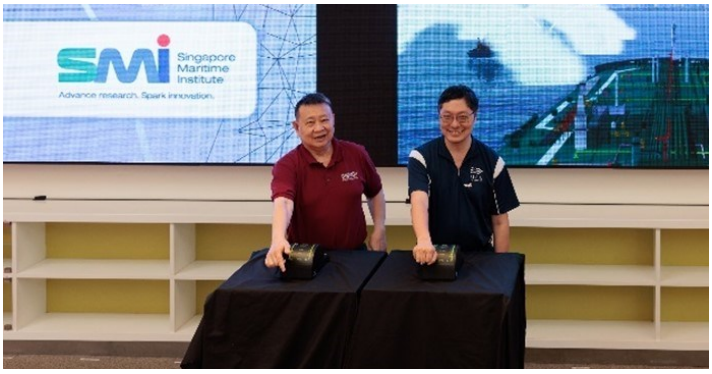

Fig 2.: Comissioning of MariOT testbed by Mr Lee Tzu Yang (left) & Mr Teo Eng Dih (right)

As a testament to the quality of the testbed, Capt Naoki Saito, ClassNK's General Manager, presented a certificate to Prof Zhou Jianying, iTrust's Centre Director, during the ceremony to certify that MariOT is in accordance with the ClassNK Cyber Security Approach. This is the first maritime testbed to be awarded with such an accolade.

Fig 3.: VIPs of the Commissioning ceremony (from left to right: COL Clarence Cai, DIS Defence Cyber Chief, Prof Lim Seh Chun, SUTD Acting Provost, Mr Kenneth Lim, MPA Assistant CE, Ambassador Chan Heng Chee, SUTD Honorary Professor, Mr Lee Tzu Yang, SUTD Chairman, Mr Teo Eng Dih, MPA CE, Prof Phoon Kok Kwang, SUTD President, Prof Lui Pao Chuen, Temasek Defence Professor, Mr David Foo, MPA Assistant CE, Mr Edward Chen, CSA Deputy CE, Prof Zhou Jianying, iTrust Centre Director, Dr Chen Xinwei, SMI Deputy ED)

Fig 4.: Presentation of ClassNK Certificate from Captain Naoki Saito (left) to Prof Zhou Jianying (right).

Following the commissioning ceremony, guests were then invited to visit the new MariOT. iTrust's Research Fellow, Dr Awais Yousaf, gave a tour of the new testbed and showed the guests the functions and capabilities of the MariOT.

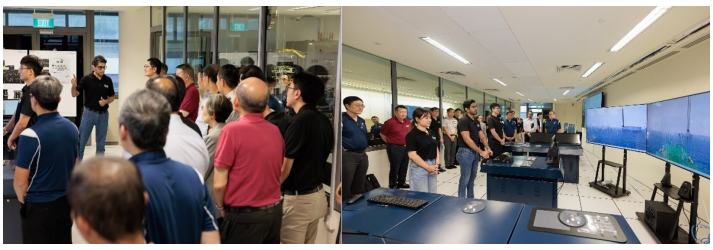

Fig 5.: Dr. Awais Yousaf hosting the tour of MariOT testbed.

The launch of the MariOT shipboard testbed marked a new milestone for iTrust. MariOT is the fourth critical infrastructure testbed hosted by iTrust since the first testbed, Secure Water Treatment (SWaT), was launched 10 years ago.

Developed in close collaboration with the MPA,

Singapore Maritime Institute (SMI) and industry partners – ST Engineering Info-Security Pte Ltd, Wartsila ANCS and ARI, MariOT is the world's first industrial grade cyber-physical simulator designed for maritime cybersecurity research, education, training and cyber exercises.

MariOT is equipped with essential shipboard operational technology (OT) systems and offers a safe and realistic testing environment for cybersecurity technologies without disrupting actual vessel operations. It will be used for in-depth research and training for academia, government agencies, and international collaborators through cyber exercises and drills, with the aim to strengthen cybersecurity resilience across the maritime sector.

SMW 2025

Visits—Singapore Maritime Week (SMW) 2025

With the commissioning of the new MariOT testbed, iTrust hosted various international and local delegates who had attended SMW as well as the Singapore Maritime Research Conference (SMRC) 2025 organised by SMI.

Fig 6.: Prof Zhou Jianying and Dr Awais Yousaf pictured with SMW delegates.

The visitors were introduced to iTrust by Prof Zhou Jianying followed by a tour to MariOT and SWaT.

Fig 7.: Prof Zhou Jianying and Dr Awais Yousaf pictured with SMW delegates. Dr Awais Yousaf showcasing the MariOT testbed to international and local delegates attending the SMRC conference.

Partnerships

iTrust Goes International

By: Aditya Mathur

The Water Tower, commonly referred to as TWT, is a premier R&D center located in Buford, Georgia, USA. Buford is a suburb of Atlanta and is about an hour drive from the Atlanta Hartfield Airport.

"The Water Tower is driven by transforming the future of water through cutting-edge research, workforce development, and global industry collaboration. As a nonprofit innovation hub based in Gwinnett County, Georgia, we bring together industry leaders, utilities, private companies, NGOs, and academic institutions to tackle the world's most pressing water challenges. Our state-of-the-art facilities, living laboratory, and extensive training programs empower the next generation of water professionals while accelerating the adoption of groundbreaking technologies. By fostering collaboration, advancing digital transformation, and bridging the gap between research and real-world application, The Water Tower is shaping a more sustainable and resilient water future - because water isn't just a resource, it's everything."—TWT web site

Thanks to TWT's CEO Melissa Meeker, in October 2024 iTrust became a research partner of TWT. A formal iTrust office has been set up by TWT in its premises. The office is self-contained and comes equipped with three large screen monitors and a desktop computer, from which iTrust can perform its work and showcase its technologies to potential licensees and interested parties.

Fig 8.: Prof Aditya pictured with Melissa Meeker, Chief Executive Officer of The Water Tower.

TWT receives live data stream from five water treatment plants that serve the population of Gwinnett County. The monitors in the office are used to display the state of any of the five plants selected via a separate screen connected to a desktop computer. Authorised iTrust researchers can view the plant state in live mode to understand their operation.

Under a non-disclosure agreement, TWT has provided a dataset sampled at a frequency of 10 minutes over 3 months. This dataset is currently in use for creating models to demonstrate iTrust technologies for detecting anomalies in large physical plants.

Dataset Milestones

iTrust and AI: The World Innovates

By: Aditya Mathur

18 March 2015 will go down in iTrust history as the day when the foundation for innovation in the design of safe and secure Critical Infrastructure (CI) was laid. At the press of a button, Professor Quek Tong Boon, then Chief Defence Scientist, started the water flowing through the first and finest of physical testbeds aimed at research, education, and training in cyber security focused on CI. During the following decade three additional testbeds were created, namely, WaDi for water distribution, EPIC for electric power, and a cyber-physical testbed, namely, MariOT, for shipping. To the best of our knowledge, SWaT-WaDi-EPIC is the first and only interconnected physical testbed of its kind in the world.

Available 24/7 with nearly no constraints on researchers on SWaT's usage, the freedom to play at will with a realistic and operational plant sprouted new ideas for CI defence. The testbed enabled intensive experimentation that led to data, analysis, and the creation of knowledge. Publications started pouring out. This was an exciting period for all in iTrust. This led to several questions. What if such testbeds are available to researchers across the world? How would that impact the security by design of CI? How to make such a testbed available remotely? It was too early to find answers to such questions. Making a prized asset accessible to others meant overcoming technical, geographical and operational challenges.

While it was decided then that even though we were unable to allow the world direct access to SWaT, we could collect datasets generated through its operation and make it public. We found support for this idea among my colleagues in iTrust. Together we decided that SWaT will be run non-stop for 11-days and the data collected. Several researchers and the engineer agreed to spend the nights in the laboratory to ensure the testbed's safe and uninterrupted operations.

Data collection began on 22 December 2015, at 4pm. A set of about 40-attacks, single and multi-point, were designed. SWaT was run with no attacks until 28 December when the first attack was launched at around 10am. Attacks were launched and removed until 2 January 2016 at about 3pm when the last attack was launched. In the end, the dataset was extracted from the SWaT historian into an Excel spreadsheet. The 125 MB file contained 54 labeled columns of sensor data in 449,921 rows. This was valuable information on the behaviour of a physical plant's actuators such as pumps, valves, and other devices. Soon the dataset, together with a list of time-stamped attacks launched, was available via a link at the iTrust website. Anyone in the world could make a request via email and get access to the data. This was the start of fulfilling a dream of enabling unfettered testbed access to scientists across the world.

Gradually researchers in machine learning started downloading data. While there were only two downloads in 2016, this quickly ballooned to 62 in 2017, 389 in 2018, and 1,591 downloads in 2019. Clearly, this amounted to an exponential growth in downloads. Researchers started submitting their work for publication citing the use of SWaT dataset. The publications from iTrust laying out the architecture of SWaT served as valuable references for researchers to relate the downloaded data to the plant processes, and activity around the SWaT dataset started to grow rapidly.

WaDi and EPIC datasets became available to iTrust researchers in, respectively, 2016 and 2017. Taking a cue from the SWaT dataset, researchers collected data from these two testbeds. These datasets were also made available on the iTrust website. Other datasets collected during cyber exercises and generated using simulation were also made available over the years. Gradually, a significant amount of valuable

information was available to researchers across the world.

In March 2025, iTrust reached a new milestone. Datasets made public by iTrust were downloaded more than 18,000 times by researchers, and reaching 100 countries for the first time. While we do not have an account of how many publications are based on iTrust datasets, we know that the publications that describe the datasets have received over 1,500 citations.

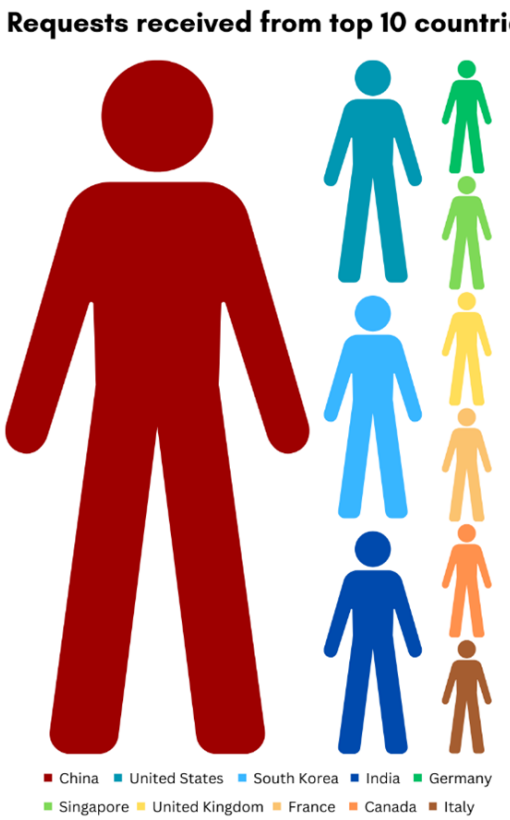

Fig 9.: [Infographic] Dataset downloads from Top 10 countries.

The dream of making the testbeds available to researchers worldwide became a reality during Covid. A team of dedicated iTrust staff worked to connect all testbeds to the Internet. For the first time in 2021, the Critical Infrastructure Security Showdown (CISS), conducted jointly by MINDEF and iTrust, became perhaps the world's first online exercise involving multiple fully physical and operational plants.

iTrust was created by SUTD and MINDEF in 2012 as center for research in cyber security. The outcomes from the researcher conducted in iTrust was intended to be made public via peer reviewed research publications. While iTrust has continued to engage in open research, the access to interconnected physical (and soon, digital) testbeds and datasets distinguishes it from among the myriads of similar centres across the world.

Though a dream is realised, much work is needed for the technology to permeate into CI. Towards this end, iTrust will continue to serve Singapore and the world by continuing on a path that aims to benefit humanity through intensive research, education, training, and technology translation.

CiMS Updates

CiMS Award Ceremony

iTrust's annual CSA-iTrust Master of Science in Security by Design Scholarship Award Ceremony awarded five outstanding students in January 2025. This scholarship recognises students who have demonstrated academic excellence, commitment, and passion for the field of cybersecurity. Our recipients were selected based on their interest and potential contributions to cybersecurity projects and their commitment to learning and manage the rigour of the MSSD coursework.

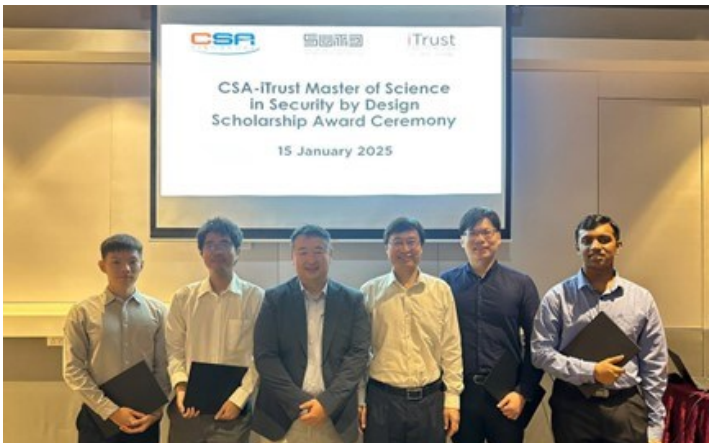

Fig 10.: Stanley Tsang, Chairman of the Governance board of Cyber Security Laboratories Singapore (second from left) and Prof Zhou Jianying (third from left) pictured with the awardees of the CiMS Scholarship (from left to right: Tan Qi Feng, Jermyn Sng Jian Min, Lee Huang Jie Belson, Madhan Selvapandian)

The ceremony also introduced an upcoming initiative on Women in Cybersecurity called "CypHER". Managed by a team of female staff and researchers in iTrust, the objective of this initiative is to support, mentor, and empower women in the cyber security field through taking up scholarships like CiMS, professional training and internships. Through this, iTrust aspires to continue contributing to the growth of the next generation of women leaders and encourage them to take bold strides in cyber security.

As cybersecurity threats continue to grow, the need for skilled professionals becomes more critical than ever.

By investing in talented students, CiMS and CypHER will play a vital role in shaping the future of cybersecurity and ensuring a safer digital world for all.

Outreach Statistics

iTrust Students Outreach Statistics

iTrust's cyber security outreach programme has continued to impact students' internship experience since the programme's inauguration 11 years ago. With more than 220 students from 47 schools hailing from 15 different countries, the programme has fostered an international network of skilled individuals, each equipped with critical cybersecurity knowledge and hands-on experience. The programme's longevity speaks to the its success in adapting to the dynamic challenges posed by emerging cyber threats and technology advancements. The programme's impact is not just limited to the personal growth of its participants; it has contributed to the broader cybersecurity community, creating a cohort of professionals in the pipeline, ready to tackle some of the most pressing cyber challenges in the world today. As it continues to evolve, the cybersecurity internship remains a key stepping stone for aspiring professionals, providing them with the tools, network, and knowledge needed to make meaningful contributions to the security of the digital landscape.

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

Manager

vanessa_lee