iTrust Times

A Quarterly Newsletter

Issue Highlights:

- CSA Academy Sing301 Training *pg. 2*
- Cyber Exercises *pg. 2*
- Conference *pg. 4*
- Visits *pg. 4*
- iTrust Anniversary BBQ *pg. 5*
- New staff: Student interns *pg. 5*

Jul — Sep 2023 | Volume 9 Issue 3

From Centre Director's Desk

Dear readers,

Greetings from iTrust!

This is the first issue of the iTrust newsletter for which I am writing a foreword. I have taken over from Prof Aditya Mathur as iTrust's Centre Director from 1 August 2023. Prof Mathur will continue to lead a few key research projects while offering support to my new role.

iTrust was established in 2013, supported by Ministry of Defence, Singapore (MINDEF). We just celebrated the 10th year anniversary on 7 July 2023. In the past 10 years, iTrust kept growing under the leadership of Prof Mathur. Today, iTrust is a well-established cybersecurity research centre in the world, focusing on Design Science and Technology for Secure Critical Infrastructure. iTrust hosts three world-class fully operational testbeds: SWaT for secure water treatment, WADI for water distribution, and EPIC for electric power. They have been used for R&D, professional training and education, cyber exercise and technology validation. They are also open to global users, with remote access via VPN, offering testbeds as a service (TaaS).

I will ride on the momentum to drive iTrust to the new heights in the next era, with the continuous support from our excellent team members as well as funding agencies and academic/industry collaborators. We will expand to the new sectors of critical infrastructure beyond water and power, and push for technology translation and commercialisation. We will seek deeper international collaborations to expand the influence and reach of iTrust.

Maritime – a key growth sector in Singapore – is the latest critical infrastructure sector iTrust has been focusing on since 2020. We have released new guidelines for cyber risk management in shipboard OT systems which can be used by authorities and shipowners to conduct cyber risk assessment. We are building a new maritime shipboard OT testbed, named MariOT, to provide a safe and realistic environment for testing and validating new maritime cybersecurity technologies before being adopted. MariOT will also be used for cyber exercise, training and education. We will give more update on maritime cybersecurity in the subsequent issues of iTrust newsletter.

iTrust has been very active in cyber exercises in operational technology by leveraging our cyber-physical system testbeds. In this issue, you will see the report of Critical Infrastructure Security Showdown (CISS) 2023, which is a premier and one-of-its-kind critical infrastructure cyber conducted jointly by iTrust and MINDEF. It offers the access to the world's largest interconnected industrial-grade critical infrastructure playground hosted in iTrust. iTrust also supports the Digital Intelligence Service in the Critical Infrastructure Defence Exercise (CIDeX) 2023 to train regulators and operators in the defence of critical infrastructures. Stay tuned.

I hope you enjoy the reading of iTrust newsletter. We also welcome the feedback and are open for collaborations.

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

Training

CSA Academy Sing301 Training

With the aim of benefiting both the local community and the broader ASEAN ecosystem, iTrust, in partnership with SUTD Academy and Tegasus International supported the Cyber Security Agency of Singapore (CSA) in the first run of its Singapore Industrial Control Systems Cybersecurity (SG-ICS301) Training. Tegasus International was the main training provider in SG-ICS301.

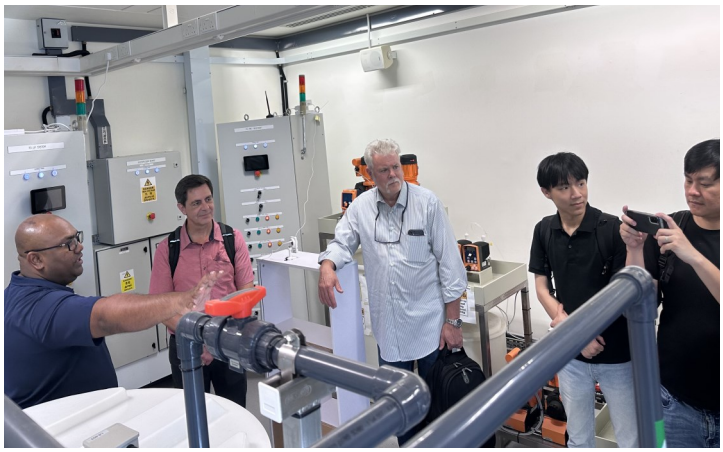

Fig 1: iTrust Cyber Engineer Aanand (left) introducing the testbeds to the SG-ICS301 Participants.

As part of the SG-ICS301 training programme, on the 23 August 2023, iTrust hosted a tour of its testbeds by comprising a cohort of trainees hailing from various ASEAN countries, as well as observers from the Cybersecurity and Infrastructure Security Agency (CISA) and Idaho National Laboratory of the United States. Prior to the tour, Founding Centre Director Prof Aditya Mathur gave an overview of iTrust to the trainees, who were undergoing the intensive week-long training programme. The tour was an integral component of the training programme as they would be utilising it for a cyber exercise later in the week.

Fig 2: Prof Adiya interacting with the SG-ICS301 Participants prior

Cyber Exercises

Critical Infrastructure Security Showdown 2023 (CISS 2023)

Critical Infrastructure Security Showdown 2023 (CISS 2023) is a premier and one-of-its-kind cyber exercise in operational technology. This international exercise is held entirely remotely and opened to invited international participants.

Fig 3: Critical Infrastructure Security Showdown 2023 (CISS 2023) Banner— Theme: Let OT Reign

The 7th iteration of CISS 2023 returned with the following bumper list of exciting additions:

- 48-hour CTF-style Stage 1: 20 challenges involving PLCs, digital twin, and a live scoreboard
- In additional to SWaT, WaDi and EPIC testbeds, a gas pipeline testbed was added.
- Additional datasets from network for network forensics and familiarisation
- More attack objectives, including an Open Category
- Novelty prizes

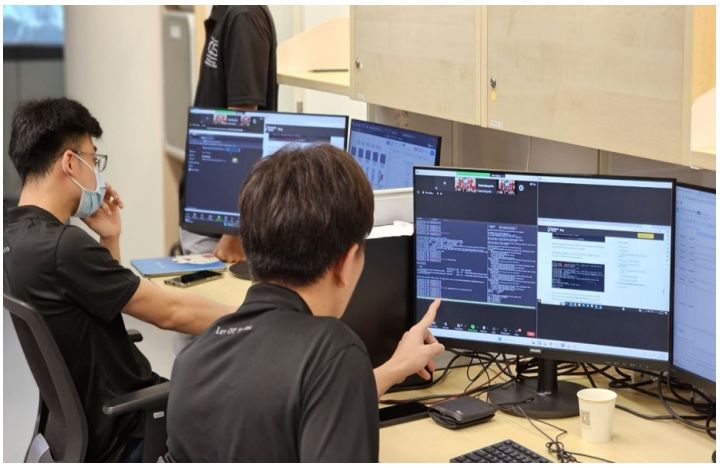

Fig 4: Green Team comprising student interns assisting judges with monitoring red teams' activities.

iTrust SUTD conducted its annual signature OT cyber security exercise - the Critical Infrastructure Security

Showdown (CISS) - for the 7th time this year with The Digital and Intelligence Service (DIS). The exercise started on 17 Aug 23 with an opening ceremony hosted by iTrust Centre Director Jianying Zhou and Commander, Cyber Defence Group, DIS, COL Shengyang Tan.

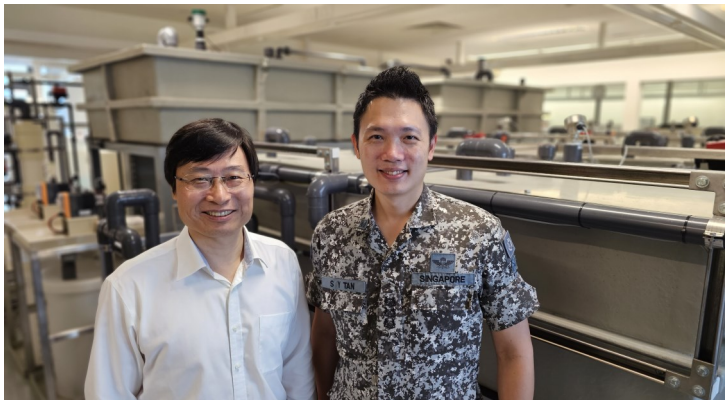

Fig 5: Prof Jianying Zhou (left) and COL Shengyang Tan at the CISS Opening Ceremony

CISS 2023 is largest instalment of ever, with a flurry of activities spread across 10 days, beginning with a massive and record number of 41 international red teams besting each other in a 48-hour Stage 1 OT-style CTF and culminating in 11 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 infrastructures.

Fig 6: CISS judges (left to right): Delaney Ng (Technical Director, SANS APAC), Miliary Expert 6 William Teo (Head, SAF Threat Hunting Centre, DIS), Matthias Yeo (CEO, CyberXCentre), Rong Hwa Chong (Director, Research and Innovation, GovTech).

At the Awards and Closing Ceremony on 28 Aug 23, iTrust Founding Centre Director Prof Aditya Mathur shared key statistics of CISS, and COL Shengyang Tan announced the top 3 red teams - Undecided (1), ADFCSA (2), and OPENEYES (3). They received cash prizes of up to S$4,000 and a limited edition CISS medallion. Congratulations!

iTrust thanks the tremendous support from the Cyber Security Agency of Singapore (CSA) for funding this annual cyber exercise, the DIS for co-organsing it, the National Cybersecurity R&D Lab (NCL) for hosting Stage 1, CISS judges William Teo, Delaney Ng, Matthias Yeo, Rong Hwa Chong for contributing their expert knowledge and the army of green team members who worked tirelessly behind the scenes to support the entire exercise platform.

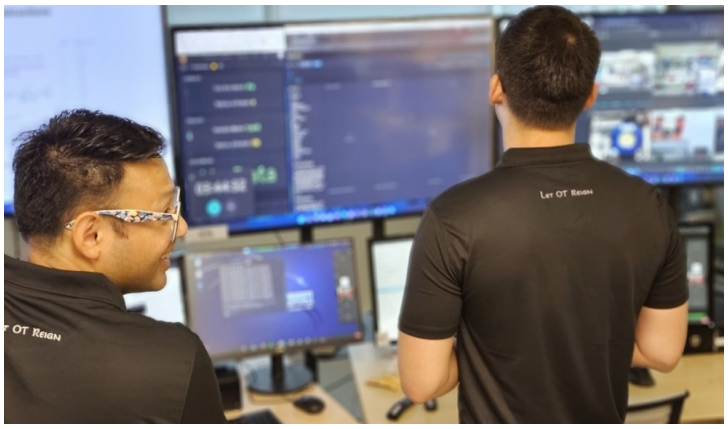

Fig 7: Cyber Tech Lead Francisco Furtado (left) and Boon Kiat Tay were the technical planners for CISS.

Critical Infrastructure Defence Exercise (CIDeX) 2023

In addition to CISS, the Ministry of Defence, Singapore (MINDEF) is also organising the Critical Infrastructure Defence Exercise (CIDeX) 2023.

CIDeX is a comprehensive cyber exercise designed to provide Singapore's critical infrastructure (CI) operators and regulators with a learning platform to understand and put into practice the defence of CI. By gaining a deeper understanding of how CI, encompassing both IT and OT networks, can be vulnerable to cyberattacks and their resulting impacts, CII teams can extract valuable insights and customize them to enhance the cybersecurity response and protection strategies within their respective organizations.

2022 recap

The 2022 Critical Infrastructure Defence Exercise (CIDeX) was the largest OT hands-on-keyboard Critical Infrastructure defence exercise in Singapore. The exercise provided a platform for Singapore's cyber defenders to train together the defence of Critical Information Infrastructure (CII).

Over 50 cyber defenders from 17 organisations representing five critical sectors — power, water, telecommunication, land transport and maritime — formed five combined blue teams to monitor and defend

the CII systems over two days. A composite red team will launch a series of live simulated cyber-attacks on these systems over two days, while the five blue teams worked in concert to detect and respond against the attacks.
A comprehensive 3-day pre-exercise training programme was conducted in SAF's Cyber Test and Evaluation Centre (CyTEC), to equip the blue teams with the capability and confidence to navigate through the CII platform and utilize appropriate cyber tools to monitor the platform and respond to the cyber-attacks.

Conference

Supergen Energy Networks Conference

iTrust Assistant Director Mark Goh and Cyber Tech Lead Francisco Furtado were invited by University of Bristol's Pro Vice-Chancellor for Research and Enterprise Prof Phil Taylor to the Supergen Energy Networks Conference in London from 5 to 6 Sep. They met with numerous experts from the UK energy sector - regulators, industry, academia - to learn how the sector is managing and mitigating cyber risks. This was a perfect platform for iTrust to make its foray into the UK energy sector and discuss with its stakeholders how iTrust can contribute to the sector. At the conference, they also had the pleasure to meet with Prof Taylor - who is also the Supergen Hub Director - and Lecturer Dr Sridhar Adepu, who was previously a PhD student and postdoc at iTrust.

Fig 8: (left to right) Dr Sridha Adepu with Mark and Francisco at the Supergen Energy Networks Conference

Prof Taylor had also arranged for Mark and Francisco to have a rare behind-the-scenes visit to Northern Powergrid's (NPG) control room on 8 Sep to learn how it manages its power grid operations. They also discussed with NPG the cyber security protocols and protection that have been put in place and how iTrust can assist in the protection of its OT assets.
Finally, Mark and Francisco also met with long-time iTrust collaborator Dr Deeph Chana on 11 Sep at Imperial College, where it houses the newly established Defence Innovation Accelerator for the North Atlantic (DIANA). Dr Chana shared how DIANA provided deep tech and dual-use innovators with access to NATO resources to adapt their solutions for defence and security needs across the NATO Alliance, and explored ways in which iTrust could contribute to DIANA's efforts.

Fig 9: (left to right) Dr Sridhar Adepu with Dr Deeph Chana and Francisco at DIANA office.

Visits

Visit by German Ministry of Foreign Affairs Chief Information Security Officer

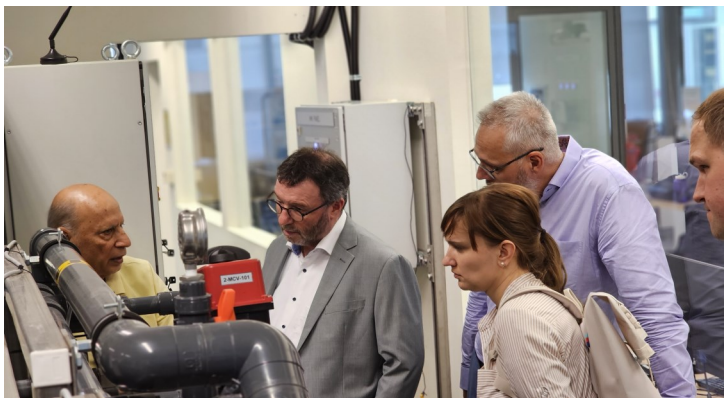

Fig 10: Prof Aditya (left) giving a tour of the testbeds to the German delegates (left to right) Mr Volker Nils Presse, Ms Birthe Peters and Mr Dietmar Hoppen, with Col Michael Maemmerer (background) looking on

The visit was organised by Col Michael Kaemmerer, who had encouraged the delegation from the German Ministry of Foreign Affairs to visit iTrust. Col Kaemmerer, the Defence Attaché to Singapore and the Philippines at the Embassy of the Federal Republic of Germany, had visited iTrust on several occasions and was impressed by how the testbeds and platforms supported the defence of critical infrastructures. During the visit, Prof Aditya conducted a tour of our advanced testbeds so that the

delegation could gain firsthand insights into iTrust's efforts in protecting critical infrastructure through R&D, technology licensing, training and cyber exercises. iTrust regularly hosts visits from local and international cyber professionals and such exchanges of knowledge and ideas is crucial in strengthening global cybersecurity efforts to build a more cyber safe world.

Celebration

Happy 10th Anniversary to iTrust!

iTrust celebrated its 10th year anniversary on 7 July 2023, surrounded by current and former staff and researchers, as well as the dedicated core team of individuals and government agencies – including those from CSA, MINDEF, PUB and SMI – who have provided unwavering support to iTrust throughout the years.

Fig 11: iTrust Cyber Tech Lead Francisco taking a Selfie with iTrust.

During the celebration, it was also announced that the founding Centre Director, Prof. Aditya Mathur, will pass on the directorship baton to Prof. Jianying Zhou starting from August 1, 2023. Prof. Mathur will continue to lead a few key research projects while offering support to Prof. Zhou in his new role. Prof. Zhou is no stranger to iTrust or the cybersecurity community, having served as the Co-centre Director for several years.

Fig 12: Prof Jianying Zhou (left) with Prof Aditya Mathur (right) cutting iTrust 10th Anniversary cake.

iTrust takes immense pride in its journey toward realising its vision of becoming the premier global centre for applied research in the cybersecurity of critical infrastructure. Here's to a new era of leadership and the anticipation of many more successful decades ahead!

iTrust Matters

New iTrust Interns

Two final year students from Temasek Polytechnic are interning at iTrust from June to December 2023, under the supervision of iTrust Cyber Tech Lead Francisco Furtado.

Jun Sheng is currently in his final year at Temasek Polytechnic, pursuing a Diploma in Cybersecurity & Digital Forensics. He is enthusiastic about learning more about Cybersecurity & Digital Forensics, as well as programming.

Since the Critical Infrastructure Security Showdown (CISS), Jun Sheng has been working on a task that involves in-depth research and reporting on MITRE Caldera, a specialized cybersecurity framework designed for automated adversary emulation, with a focus on testing and evaluating network defenses. His responsibilities have encompassed the deployment of Caldera and conducting thorough testing to gain insights into its capabilities, limitations, and potential applications.

Throughout this process, Jun Sheng drawn upon his prior experience with Caldera and supplemented it with valuable online resources. The primary objective of his project is to assess whether MITRE Caldera could prove to be a valuable asset for iTrust. In pursuit of this goal, he conducted independent research, explored various testing scenarios, and honed his ability to adapt and troubleshoot in real-world cybersecurity contexts.
Jun Sheng feels that this journey of discovery and problem-solving has been a captivating and enriching experience. He is currently in the process of crafting a presentation based on his findings, which will serve as a means to evaluate the potential utility of MITRE Caldera for iTrust.

Rian is a final year student of Temasek Polytechnic specialising in Cybersecurity and Digital Forensics,

now an intern with iTrust. He is interested in IoT, cybersecurity and machine learning.

Since the Critical Infrastructure Security Showdown (CISS), he has been working on a task that involves researching and reporting on MITRE Caldera, a cybersecurity framework that specializes in automated adversary emulation for testing and evaluating network defenses. Rian's tasks have included deploying Caldera and conducting comprehensive testing to understand its capabilities, limitations, and potential use cases. Throughout this process, he leveraged his experience working with Caldera and supplemented it with valuable resources he found online.

The primary objective of this project is to evaluate whether MITRE Caldera could be a valuable asset for iTrust. To achieve this, Rian conducted independent research, experimented with various scenarios, and learned to adapt and troubleshoot in real-world cybersecurity contexts. This ongoing journey of discovery and problem-solving has been both interesting and enjoyable for Rian, and he looks forward to sharing the results with the team in due course.

LinkedIn

iTrust is now on LinkedIn — connect with us! Feel free to reach out to us to explore research collaborations, testbed usage and training and testing services.

General Enquiries

iTrust: *itrust*

NSoE: *nsoe_destsci*

CiMS: *cims*

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

Scan to view previous publications.

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

Francisco FURTADO
Cyber Tech Lead, iTrust
francisco_dos

Mark GOH
Assistant Director, iTrust
mark_goh

iTrust Laboratories

Andrew TAY
Research Senior Technologist
andrew_taykongngee

TAY Boon Kiat
Cyber Security Technology Engineer
boonkiat2_tay

Aanand R
Cyber Security Technology Engineer
Aanand_r

National Satellite of Excellence

Jillian CHIN
Manager
jillian_chin

Angie Ng
Manager
angie_ng

Siti Nadhirah Shaik NASAIR
Snr Research Associate
siti_nadhirah

Vanessa LEE
Deputy Manager
vanessa_lee