# iTrust Times

A Quarterly Newsletter


Issue Highlights:




*Picture credit: NATO CCDCOE*


**Apr—Jun 2021 | Volume 7 Issue 2**


From Centre Director's Desk

## Exercise Is Good For You

Dear Reader:

Greetings from iTrust!

This year started with yet another first for iTrust: participation in the world's largest live-fire cyber security exercise, namely Locked Shields (LS2021), organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). This was the first time the exercise was online and also the first time that iTrust contributed a system – in the form of a digital twin for water treatment – and manpower to it. A total of 26 instances of the twin, named "Berylian Water Purification Plant," were installed at the CCDCOE IT infrastructure. The CCDCOE red team, supported by iTrust, launched attacks on the twin while the blue teams from NATO countries defended the plant. The NATO blue teams were supported by an iTrust green team. iTrust's participation was made possible by MINDEF, who funded our efforts and provided the much needed manpower to support the red and blue teams and installation of the twin. Additional information regarding LS2021and the twin is in this newsletter.

As I write this forward, I cannot but mention the two most serious successful cyber-attacks on critical infrastructure in the US. The ransomware attack on Colonial Pipeline led to the shutdown of its distribution infrastructure. The pipeline operation resumed after a US$4.5M ransom was paid to the attackers (perhaps some of the ransom has been returned.) Another successful ransomware attack on the world's largest meat plant (JBS) led to the stoppage of its production facilities.

iTrust researchers focus exactly on extreme attacks similar to the ones mentioned above that lead to service disruption and plant damage. The sole aim of iTrust technologies, such as SafeCrit that includes PlantProtect, is to rapidly detect process anomalies and prevent damage by identifying rogue commands sent to plant actuators. The use of iTrust technologies prevents, or reduces the chances of, attackers to take control of the physical processes in a physical plant. Thus, while an attacker may compromise, for example, a billing system in a plant, they will be prevented from actually controlling the plant's physical processes when the billing system is not connected to on the plant network . iTrust is currently in talks with companies in Singapore and US for piloting its technologies at different physical plants. Upon successful pilots, I hope that the technologies will be installed in

plants on which depend the daily lives of millions of people.

Another newsworthy item from iTrust is the Fifth Critical Infrastructure Security Showdown 2021 (CISS 2021-Online) scheduled for 6 to 17 September. The exercise this year will be the largest ever involving two live critical infrastructure systems and two digital twins. These systems will be attacked by red teams and defended by the blue teams. iTrust technologies will be once again put to extensive testing during the exercise. The exercise is organised jointly with Singapore's Ministry of Defence and will feature a number of invited blue and red teams from various countries.

I hope you will enjoy reading this issue of the newsletter.

Best wishes and regards.

Aditya Mathur
Centre Director, iTrust, SUTD
Director, National Satellite of Excellence DeST-SCI
Professor Emeritus, Computer Science, Purdue University

Research Focus

LOCKED SHIELDS 2021

Exercise Locked Shields: 22 Blue Teams defending against over 4,000 cyber-attacks in what is dubbed as the largest and most complex international live-fire cyber defence exercise in the world. The annual cyber exercise, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), stretched over two intense days where the blue teams, comprising NATO member nations and partners of CCDCOE, practiced the defence of national IT systems and critical infrastructure (CI) in the event of a large-scale cyberattack.

As a Centre for Research in Cyber Security at SUTD specialising in the safety and security of CI, iTrust contributed to one of the CI platforms used in the exercise. A digital twin of iTrust's Secure Water Treatment (SWaT) testbed – the SWaT digital twin – was replicated across 22 systems (Figure 1) to enable each Blue Team to defend it independently against the Red Teams' attacks. Not only was the first time iTrust could actively contribute to Exercise Locked Shields, it was also the first time the SWaT digital twin was used on such an international scale.


***Fig 1: An organiser briefing members on the SWaT digital twin used by the Blue Teams***


**Bigger, better**

iTrust's annual signature cyber exercise, CISS2021-OL, returns this year with a bang. Co-organised with Singapore's Ministry of Defence (MINDEF) and supported by the National Research Foundation (NRF) and Cyber Security Agency (CSA), CISS2021-OL will see the retention of the online platform modality, with the following exciting additions for Red Teams:

- World Wide Web as entry point to platform
- Water Distribution (WADI) testbed as the additional attack surface
- Additional 1 hour for Red Teams to launch attacks
- Intrusion Detection Systems (IDS) installed
- Higher score when a reflector server is used to mask identity

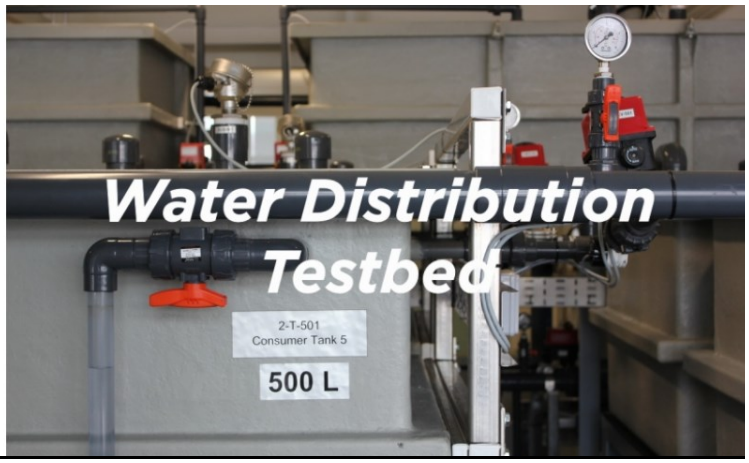




*Fig 2: Participants will have access to world's largest industrial-grade critical infrastructure playground*

- Higher score for successfully avoiding detection by IDS
- Prize award doubled

In addition to the Secure Water Treatment (SWaT) testbed, we are bringing in its sister testbed, WADI (Figure 2), to expand the playing field for Red Teams. Along with it comes additional attack objectives and surfaces for Red Teams to exploit, packaged in a novel and complex OT system (Figure 3).

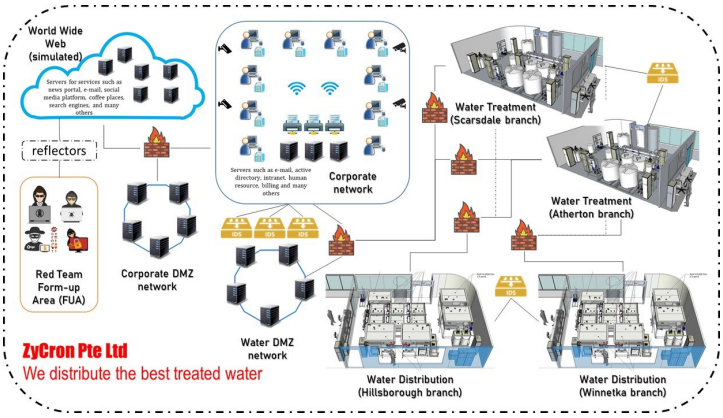



*Figure 3: System architecture this year's CISS*

iTrust also thanks the Fortinet, Gigamon and Tegasus as sponsoring partners for this year's exercise.

## Secure Water Treatment (SWaT) Digital Twin

*By Prof Aditya Mathur, Centre Director, iTrust*

The SWaT plant at iTrust is used extensively by iTrust researchers in Singapore and their collaborators around the world. Given that SWaT is a physical plant, it becomes challenging to schedule multiple researchers to use the plant. A more critical issue arises when multiple defenders are to defend the same plant at the same time. The SWaT digital twin was designed to overcome these limitations of the physical plant. This article offers a quick overview of the twin.

**Architecture:** "SWaT Digital Twin," referred to as the "twin," is a digital version of the SWaT plant located in iTrust. As illustrated in Figure 4 on the next page, the twin mimics the SWaT architecture. It contains one process for each PLC, RIO and actuator. A SCADA process controls the entire twin. All processes are independent and can run in one or more virtual machines. The twin can be run at the same speed as SWaT, which publishes its state information once every second or speeded up to 100 times. This feature enables researchers to collect large amounts of state information in a short time — which cannot be done in the physical SWaT.

**Communication architecture:** As shown in Figure 4, the twin uses ZMQ and OPC protocols for communications. When operating in the "ZMQ" mode, all communications are in ZMQ. When running in the "OPC" mode, the PLC-PLC-SCADA communications use OPC while the remaining use ZMQ. The twin publishes its state as dictionary once every plant-second. Various plug-ins connected to the twin can use this state to perform their desired functions. In its current version, the twin is interfaced to two anomaly detectors, namely AEGIS and AICrit, that are developed by iTrust researchers.

**Human Machine Interface (HMI):** A professional HMI (Figure 5) runs independently and displays the current state of the twin. Unlimited instances of the HMI can be

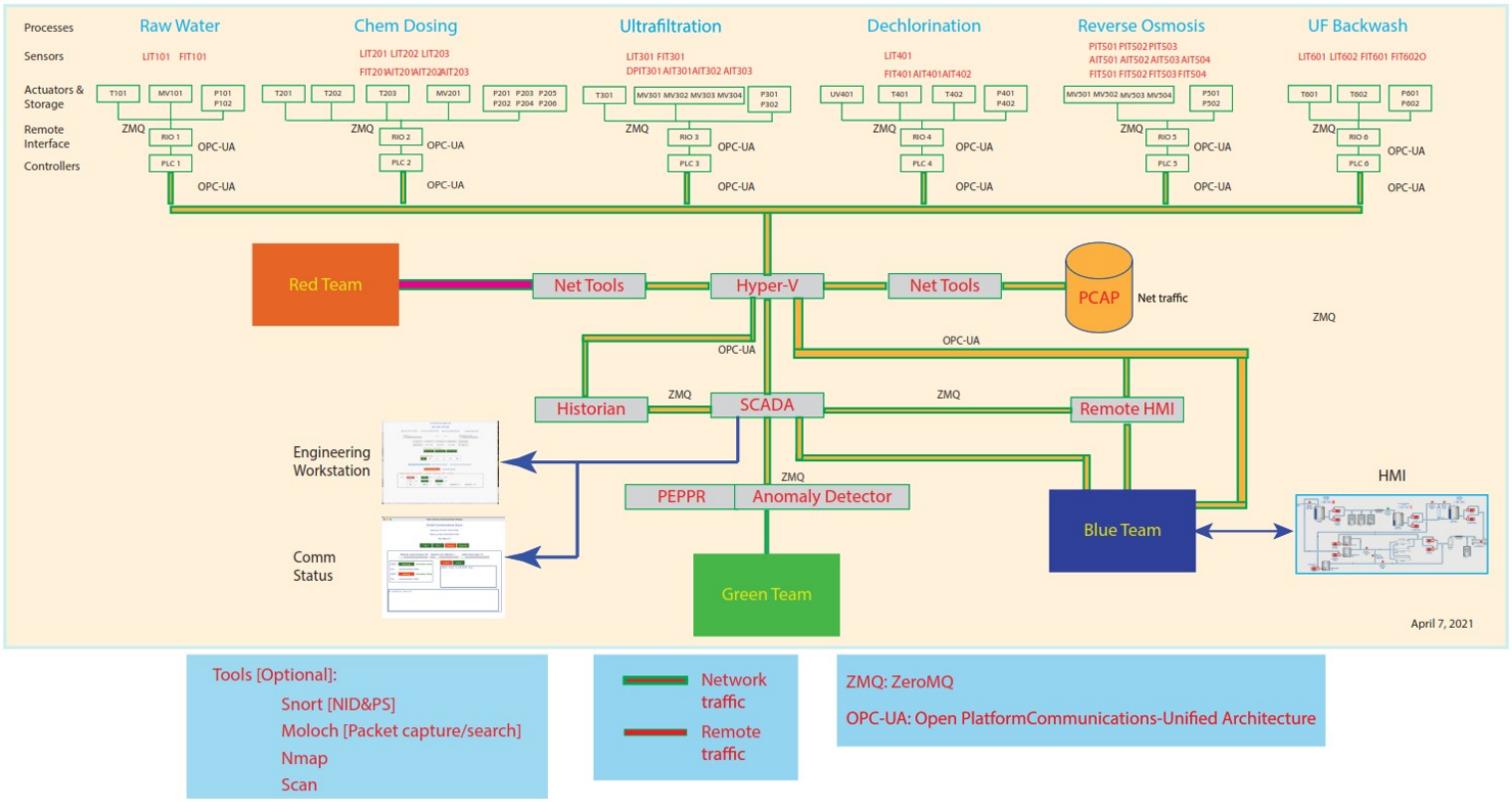



***Fig 4: Process architecture of the twin***

created to communicate with the twin. This design enables the twin to be used simultaneously by multiple defenders (blue teams) and attackers (red teams) during cyber exercises. While the primary control of the twin resides with the twin operator at the SCADA UI, control can be passed to any one of the multiple HMIs. Thus, given the two-way interface of the HMI, and when granted permission, it can be used directly to control the twin.

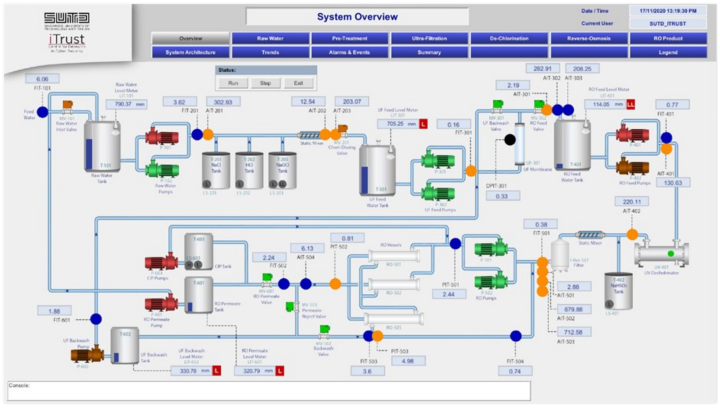



***Fig 5: HMI of the twin***

**Twin virtualisation:** The twin can be run in monolithic or distributed mode. In the monolithic mode, all twin processes are running under a single OS. In the distributed mode, various twin processes are in their own VMs that communicate over a network. Distribution of the twin allows attacks to be launched via the network to mimic those in a commercial plant.

**Attacking the twin:** In the monolithic mode, the twin can be attacked directly from any of the interfaces available. For example, a pump can be turned on or off directly via the SCADA UI, or indirectly from an HMI. In the distributed mode, the attacks can be launched via the communication network as well as via the SCADA and the HMI. This flexibility enables the twin to be configured by researchers as needed. An independent attack desk is also available that allows the design and launch of attacks via the network.

**Twin use:** The twin was first used in the Locked Shields (LS2021) exercise organised by NATO CCDCOE in April 2021. For this exercise, a special 3-stage twin was prepared from the 6-stage twin. 26 instances of the 3-stage twin were launched on different VMs. Each twin was attacked independently by a red team. Each blue team had access to three identical HMIs, with one serving as the master controller. Members of each of the 26 blue teams were able to visualise and control the twin via the HMIs.

**Twin development and the team:** Initial development of the twin was a solo effort that lasted about 2 years. Sometime in late 2020, a fully working 6-stage twin was available and demonstrated. Additional developers were added to the twin team to prepare

the twin for use during the Locked Shields exercise. iTrust researchers Francisco Furtado added the OPC protocol while Siddhant Shrivastava and Chow Wong Chong created the professional HMI. Ivan Christian created a Historian that records twin state for future analysis. Mohammad Syuqri created a visualisation tool for real-time plot of plant state variables. Gauthama Raman and Surabhi Athalye created process anomaly detectors. iTrust interns, Nicholas Png, was responsible for creating multiple instances of the twin and creating the fully distributed version during LS2021, while Sze Shao Hong created the attack desk to design and launch cyber-attacks.

**Future of the twin:** The full 6-stage twin is currently undergoing enhancement and testing. Modbus protocol is being added for communications between the RIOs and the actuators. Other commercially-used protocols will be added in the future. Being an an excellent educational and research tool, iTrust is considering making the twin available to our partners for non-commercial uses; the twin can also be licensed from SUTD for commercial use.

The entire twin development effort has been funded by the National Research Foundation and the Ministry of Defence, Singapore. iTrust wishes to thank these agencies for their continued support in its efforts.


*By Senior Research Assistant Priyanga Rajaram*

Over the years, the maritime industry has been increasingly adopting ICT for better operational efficiency. But due to the increase in the connectivity between OT and IT systems, cyberattacks in the maritime industry have been increasing as hackers try to exploit the vulnerabilities in shipboard systems. It is thus crucial that the maritime industry is aware of the cyber risks and appropriate mitigation measures to minimise its exposure to the impacts of such risks. In view of this, the Singapore Maritime Institute funded iTrust a research study titled "A Cyber Risk Management Study in Shipboard OT Systems." The study's principal investigator is iTrust Co-centre Director Prof Jianying Zhou. He is assisted by senior research assistants Priyanga Rajaram and Ruchitha Dumbala, with iTrust senior manager Mark Goh contributing as a subject matter expert.

On 18 Dec 2020, iTrust organised a webinar to share the team's initial findings on the study of shipboard OT systems and their cyber risks. The next part of the research was to **review existing guidelines and mitigation measures for shipboard OT cyber risks.** The team organised a second webinar to share its findings on 1 Apr 2021. After a welcome remark from Prof Aditya Mathur and an introduction by Prof Zhou, Priyanga presented the findings from the review, which included reports published publicly by various institutions and maritime organisations such as the International Maritime Organisation, American Bureau of Shipping, Baltic and International Maritime Council, Institution of Engineering and Technology, DNV, and European Network and Information Security Agency. Senior Research Assistant Ruchitha Dumbala then presented the **mitigation measures** that need to be implemented to tackle the risks identified (Figure 6, next page) in the four OT systems, namely, Communication systems, Propulsion, Machinery & Power Control Systems, Navigation Systems, and Cargo Management Systems.

The team then hosted a 30 minute Q&A session to take questions from the audience. As with the first webinar, the second one also generated a lot of interest, with **nearly 200 participants** from around the world. The slides and video of the presentation can be downloaded from iTrust's website. The next webinar to wrap up the study is scheduled for Aug 2021, where the team will present **a checklist of mitigation measures against cyber risks for** maritime authorities and ship owners to conduct cyber hygiene checks and a **security tier system** for ship owners to determine their level of cyber-preparedness.

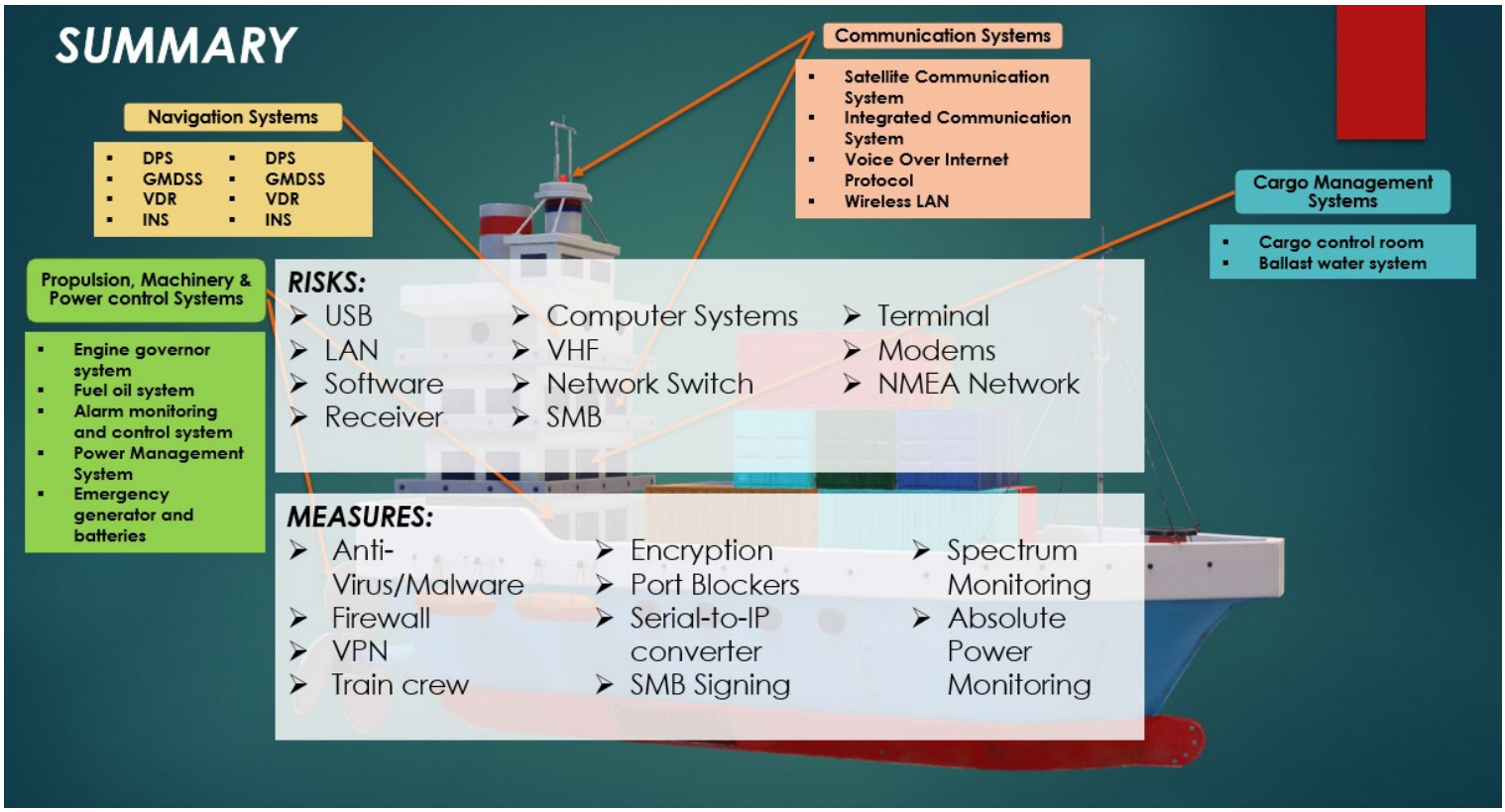



*Fig 6: Summary of shipboard OT systems and their corresponding risks and mitigation measures*

## Awards


For his contributions to energy efficient wireless communications, Associate Professor Yuen Chau has been elevated to **IEEE Fellow, Class of 2021.**

Associate Prof Yuen, a faculty with SUTD's Engineering Product Development pillar, was also awarded the IEEE Vehicular Technology Society (VTS) Distinguished Lecturer (DL) and IEEE VTS Singapore Chapter Outstanding Service Award in 2020 and 2019 respectively.

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest technical professional organisation dedicated to advancing technology for the benefit of humanity. Less than one-tenth of one percent of the total IEEE voting membership is bestowed the prestigious honour of the IEEE Fellow each year.

Congratulations, Dr Yuen!

## Visits

**Ms Aileen Chia**, the Director-General (Telecoms & Post) and Deputy Chief Executive, Connectivity Development & Regulation of the Infocomm Media Development Authority (IMDA) visited iTrust on 30 Mar 21 to learn about the centre's research work and how they contribute to the security of critical infrastructure. iTrust Centre Director Prof Aditya Mathur gave an overview of iTrust. He fielded questions relating to R&D translation projects awarded to the centre and the cyber exercises that iTrust conducted and supported throughout the year. During the exchange, they also explored ideas how a **5G testbed could be used to improve cybersecurity in the** telecommunications industry. The visit was wrapped up with a tour to iTrust's four testbeds.

*Fig 7: Prof Mathur with Ms Chia (extreme right) at WADI testbed*

Three Cyber Security Technology Engineers (CSTE) joined iTrust over the past 6 months. In addition to managing the day-to-day operations of iTrust's four testbeds, the CSTEs will also assist with research, training and cyber exercises. Welcome!

**Mavis Ang**

Mavis graduated from the Murdoch University in 2020 where she studied Cyber Security and Forensics and majored in Business Information System.

Upon graduation, Mavis worked as a Cyber Security Engineer in SAF Cyber Defence Test and Evaluation Centre (CyTEC) under NCS Pte Ltd where she oversaw the deployment and dashboard design of their SIEM tools based on the requirements stated of each exercise.

Keen to gain more exposure and experiences, Mavis joined iTrust as a Cyber Security Technology Engineer in Dec 2020.

**Andrew Tay**

Andrew previously worked in ST Engineering where he was seconded to Cyber Defence Test and Evaluation Centre (CyTEC) at Stagmont Camp as a Facility Manager since September 2012.

His main responsibilities included handling of Land and Buildings Inspection (LBI), ensuring physical security and fire safety are complied with all mandatory fire safety requirements and regulations set by SCDF, CyTEC compliance and MSD security guidelines.

Other parts of his scope included setting up the integration testing environment and infrastructure according to test scenarios, wireless communications system and simulation.

Andrew enjoys travelling and doing sports during his free time.

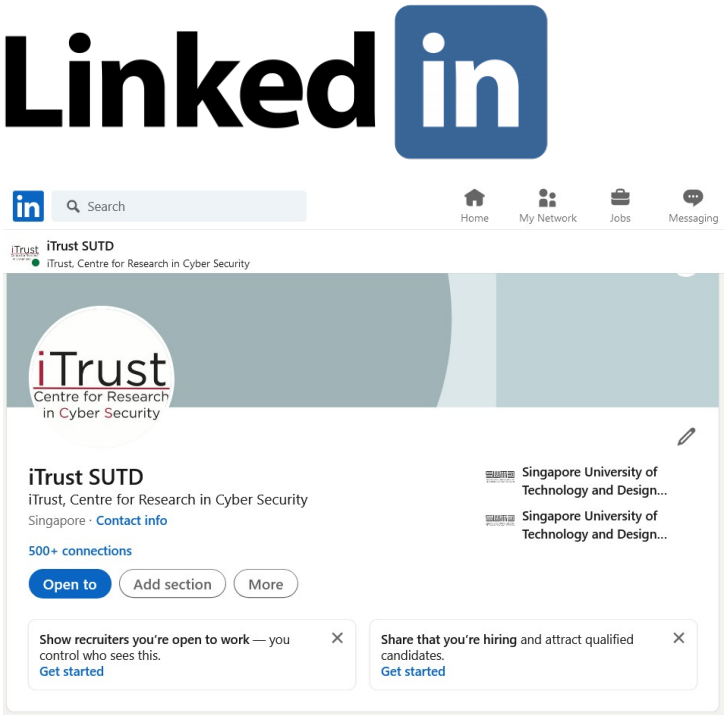
**Tay Boon Kiat**

Boon Kiat previously served in the Singapore Armed Forces as a Military Intelligence Expert Engineer (MIEE) from July 2013 till June 2021. He also graduated from Singapore University of Social Sciences with a bachelor's degree in Information and Communications Technology in Oct 2019.

In his military service, Boon Kiat was involved in the facilitation of the 3rd Generation of SAF operations and beyond. His latest field of expertise in the SAF focused on SATCOM technologies and Very Small Aperture Terminal deployments.

He hopes to meet and conquer new challenges in the increasingly prevalent world of Cyber Security.
In his downtime, Boon Kiat is an avid reader of fantasy fiction and a gaming fiend on his computer.

Boon Kiat joined iTrust as a Cyber Security Technology Engineer in June 2021.




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

## Management

**Prof. Aditya P MATHUR**
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
*aditya_mathur*

**Prof. Jianying ZHOU**
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
*jianying_zhou*

**Ivan LEE**
Deputy Director, Cyber Security Technologies
*ivan_lee*

## National Satellite of Excellence

**HOR Miao Yun**
**Research Senior Officer**
*miaoyun_hor*

**Siti Nadhirah Shaik NASAIR Johar**
Research Associate
*siti_nadhirah*

**Angie NG**
Manager
*angie_ng*

**Priscilla PANG**
Manager
*priscilla_pang*

**General Enquiries**
*nsoe_destsci*

## iTrust Laboratories

**Mavis ANG**
Cyber Security
Technology Engineer
*siewting_ang@sutd.edu.sg*

**Mark GOH**
Senior Manager
Editor, iTrust Times
*mark_goh*

**Andrew TAY**
Cyber Security
Technology Engineer
*andrew_taykongngee*

**TAY Boon Kiat**
Cyber Security
Technology Engineer

**General Enquiries**
*itrust*

iTrust
Centre for Research in Cyber Security