iTrust Times

A Quarterly Newsletter

Issue Highlights:



Apr—Jun 2019 | Issue 1

From Centre Director's Desk

## A New Beginning

Greetings from iTrust! And welcome to the 1st issue of the revamped iTrust Newsletter!

Let me begin by sharing two pieces of important news items. First, the National Research Foundation (NRF) has set up a National Satellite of Excellence (NSoE) in conjunction with, and anchored at, iTrust. NSoE at SUTD is the result of several years of hard work by faculty, research staff, students, and administrative staff in creating and nurturing iTrust.

The theme underlying NSoE is "Design Science and Technology for Secure Critical Infrastructure," or DeST-SCI in short. This recognition from NRF comes with a 3-year research grant to be managed by iTrust NSoE. The key thrust areas in DeST-SCI include: Automatic generation of detectors and command validators; Incidence response: Forensics and recovery; Attestation and assessment; Digital twinning; Attack prevention; and Novel Approaches to Design Secured Critical Infrastructures. NSoE DeST-SCI has issued a grant call to all eligible organisations in Singapore. Details are available at the following site: https://itrust.sutd.edu.sg/nsoe-destsci/grant-2019/

The second key news item is a 5-year grant from NRF to support iTrust Labs. This grant will enable iTrust to manage the four world-class testbeds in the areas of water treatment, water distribution, electric power, and IoT. Funds are also provided to conduct security assessments and create a benchmark of attacks on Critical Infrastructure (CI). iTrust Labs also includes four training platforms specifically designed for hands-on learning in the area of Cyber Physical Systems. These platforms offer PLCs and other control equipment from Allen Bradley, National Instruments, Schneider Electric and Siemens.

Infrastructure in iTrust Labs is available for public use for research, training and technology assessment. iTrust Labs will be the creator and distributor of datasets that enable research aimed at the development of new methods and tools for the design of secure CI. At the time of writing this letter, over 350 researchers from 47 countries have downloaded datasets created in iTrust Labs. Details of iTrust Labs are available at the following site: https://itrust.sutd.edu.sg/itrust-labs-home/

Some of you may know about the Secure Cyber-Physical (SCy-Phy) Systems Week and the associated SWaT Security Showdown (S3) event that iTrust has organised twice. The next round of SCy-Phy is scheduled for the week of August 26, 2019. During this week S3-19 will

aim at the assessment of commercially available technologies developed for anomaly detection and anomaly avoidance. The event will feature vendors of security technologies for CI, white hatters and observers. iTrust researchers have also developed advanced tools, to be used during S3-19, for launching attacks at various levels in a realistic CI platform: independently or simultaneously directly via the SCADA workstation, HMI, and Remote I/O as well as indirectly through the new Cyber City platform developed in iTrust.

For the first time during S3-19 two newly developed visualisers will be available to observers to watch in real time the launch of cyber attacks, the performance of the anomaly detection and avoidance technologies and the plant behaviour under attack. The Plant Visualiser provides a real-time graphical view of the current and predicted values of the plant state variables selected by the observer. Another visualiser, named VVATER, is a fully functional VR system that connects to the plant under observation. VVATER enables plant observation in real-time as well as launch of attacks on the plant. These two visualisers will bring a sense of realism to the entire S3-19 exercise.

As you may imagine, I am excited about the future of iTrust. I hope that NSoE will enable hardening of existing technologies developed in iTrust, and the development of new technologies that will be tested, and possibly deployed, in operational plants.

That's all for now folks! I end this forward with sincere thanks to all faculty, staff, and students who have participated in making iTrust an internationally recognised centre that focuses sharply on the design of secure critical infrastructure. Thanks for browsing this newsletter! We would love to hear from you (itrust@sutd.edu.sg).

Best wishes,

Aditya Mathur
Centre Director, iTrust, Singapore University of Technology and Design
Director, National Satellite of Excellence DeST-SCI
Professor of Computer Science, Purdue University

# iTrust: The first 5 years

**Look how far we've come**

From a young research centre holding its head above water in 2013 to an established cyber physical system (CPS) research centre pulling its own weight 5 years later, iTrust's achievements have remarkedly exceeded our own expectations. Here we look back at some of our proudest moments:

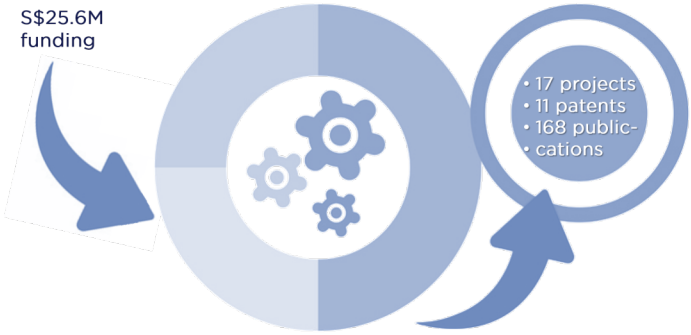


***Fig. 1: I/O - A total of $25M funding for projects has translated into numerous patent applications and publications***


***Fig. 2: Not only publications, but also awards and recognition for the high quality work produced as well***

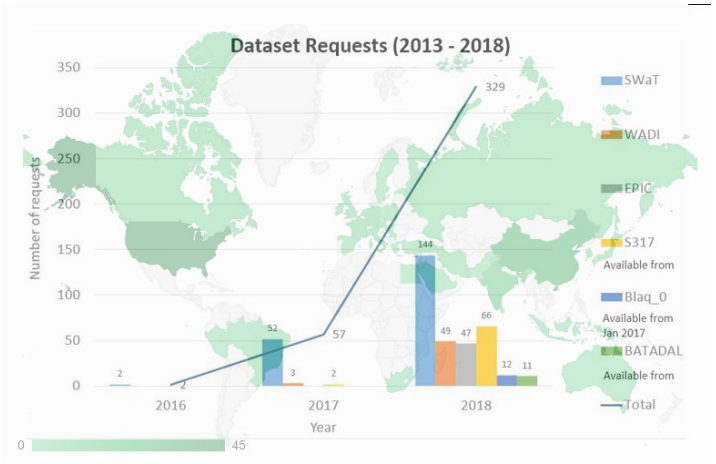


***Fig. 3: Sharing is caring - trove of data generated from iTrust's testbeds is shared with researchers all over the world***


***Fig. 4: Truly global - our researchers, interns and visitors hail from over 30 countries***

As we move to the sixth year, iTrust also secured an additional S$17.2M funding from NRF to support research and testbed operations (see following article), bringing the total research funding to nearly S$43M.

## iTrust Laboratories @ Singapore

**A 5-year grant to support iTrust's testbed operations was approved on 1 Feb 2019**

In 2015, the Secure Water Treatment (SWaT) testbed sprung up as the first testbed to support applied research at iTrust. Drawing more curious visitors than serious researchers during its infancy, SWaT has matured to become the go-to site for experiments, research, training and proof-of-concept demonstrations for many around the world.

In the meantime, three additional testbeds - power grid, water distribution and Internet of Things - blossomed over two years to add to the "garden of testbeds" from which more ideas flowered and achieved fruition. Word of the testbeds quickly spread to many research institutions and companies worldwide, with many keen to collaborate at different levels.

***Fig. 5: A garden of testbeds at iTrust***

On 1 Feb 2019, the National Research Foundation (NRF) generously **awarded funding S$4 million to iTrust** continue our research in security for cyber physical systems (CPS). The funds will allow us to extend the lifespan of the testbeds and upgrade components to support more complex and realistic research. This will help iTrust to attract world renowned researchers to work with us and help cement it as the leading CPS research centre.

iTrust aims at being a leading international centre for multi-disciplinary research in design science and technologies that enables the creation of Secure Critical Infrastructure highly resilient to cyber-physical attacks. The technologies created will be scalable for application in both new and existing Critical Infrastructure. To achieve a measure of self-sustainability, we have opened up our testbeds for rental to interested parties for research, experimentation, training and testing.

## NRF Satellite of Excellence (NSoE) in the Design Science and Technology for Secure Critical Infrastructure (DeST-SCI)

DeST-SCI National Satellite of Excellence
Design Science and Technology for Secure Critical Infrastructure

**iTrust is now a satellite with a $13M R&D kitty to fund research in critical infrastructure security**

On 15 Mar 19 iTrust was further awarded a **S$13.2M research grant by NRF** to set up an NRF Satellite of Excellence (NSoE) in the Design Science and Technology for Secure Critical Infrastructure (DeST-SCI) programme. The satellite will foster partnerships with researchers from educational institutions and with government and commercial organisations in Singapore to conduct foundational research leading to technologies for potential deployment in Singapore and its partners.

Research in NSoE will focus on creating prototypes of process centric anomaly detection systems with integrated command validators, digital twin, methods for attack response and rapid recovery from attacks, detecting code replacement in controllers, and control models using machine learning techniques for reconfig

urable control. This will be done through a **Call for Proposals (CFP)** to solicit research ideas from local research institutes in collaboration with industry.

Close partnership with owners, operators, stakeholders, and research entities focused on critical infrastructure (CI) in Singapore and various commercial stakeholders will enable moving the prototypes and methods created into actual use in operational plants. Such transfer of technology via startups will lead to highly resilient CI in Singapore, and at the same time, build manpower capability and develop expertise in CI security.

An information session on this new setup was held on 3 Apr 19 at the Singapore University of Technology and Design (SUTD). iTrust Co-Centre Director Prof Jianying Zhou announced the newly setup NSoE and briefed on the CFP to invited parties. **Important dates of the CFP and grant quantum** can be accessed at the following website: https://itrust.sutd.edu.sg/nsoe-destsci

*Fig. 6: NRF's Senior Deputy Director, Cybersecurity R&D, Ms Karen Teh delivering the opening address at the info session*

Research Focus

## iTrust Cyber City

**By Ivan Lee, Deputy Director, Cyber Security Technologies**

Few years ago, while planning for the next capability for iTrust, I came across impressive platforms from The Department of Homeland Security (DHS) in Idaho, US, and those used by the NATO Cooperative Cyber Defence Centre of Excellence's (CCDCOE) Lockshield annual exercise in Estonia. While many others focused on building cyber ranges, I was strategising for something larger and more realistic, and one that leverages on iTrust's

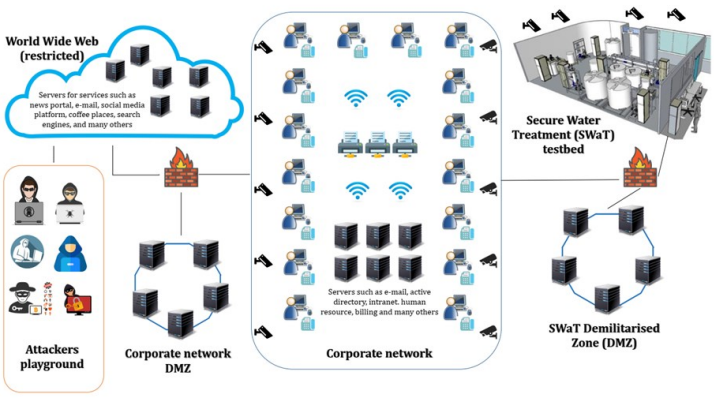


*Fig. 7: High-level Architecture of Cyber City*

existing operational infrastructures such as the SWaT and EPIC testbeds. This led to the birth of the iTrust **Cyber City that integrates the gamification element from DHS, cyber exercise element from CCDCOE, and mechanisms from other institutions.**

Holistically, the design was meant to produce an operational scaled-down version of major entities that exist in the Singapore ecosystem and construct a hybrid and representative platform consisting of virtual and physical entities for cyber security research, experimentation, training, and exercises. To realise this vision, I built a cyber organisation named "ZyCron" whose core function is operating water treatment activities in a Cyber City. ZyCron is a full-fledge organisation comprising of Information Technology (e.g., e-mail server, file server, printer server, CCTV, honeypot and intranet) and Operational Technology (water treatment processes in SWaT), that are meaningfully represented. To make these entities "alive," various types of network traffic are carefully crafted and included in Cyber City.

To make it a realistic city's infrastructure, I plan to include EPIC's power generation, transmission, distribution and grid functions in Cyber City as a separate cyber organisation. Gradually, additional realistic Critical Information Infrastructure (CII) testbeds will be integrated and the cascading relationships will become more apparent. All these CII will be interconnected through its own restricted World Wide Web where social entertainment and digitalisation platforms will be created to co-exist in the ecosystem. Taking Cyber City a step further, this entire platform can be used as a complex and large scale "honeycity" that is opened up to Shodan and darknet for in-depth research and analysis.

# SWaT Plant Visualiser (PlantViz)

**By Muhammad Syuqri & Francisco Furtado, Research Assistants**

Over the years, researchers in iTrust have used various defence techniques to develop a variety of novel anomaly detection mechanisms (ADM). These detection mechanisms include Distributed Attack Detection (DAD), Generalised Auto-Regressive model with eXogenous input (GARX), noise-based detection (NoisePrint), and various models using AI techniques. With each ADM, a separate Graphical User Interface (GUI) is usually designed to assist operators in making sense of the information received from the operational plant as well as the ADMs.

To consolidate the GUIs of the individual ADMs, we have developed **SWaT PlantViz, an integrated and feature-rich GUI for current and future ADMs.** PlantViz is a robust and dynamic web application that enables users to view the state of the plant in real-time as well as the anomalies detected by the ADMs registered with the visualiser. Features in PlantViz are summarised below.

### Multiple data sources

The default data source is the Operational Historian in SWaT testbed, which receives measurements from sensors in real-time. Users are also able to retrieve historical data sources such as CSV files containing past measurements.

### Multi-plot and predicted values for tags

The GUI can accommodate up to four subplots. This allows users to monitor and focus on a specific stage of the plant network, or multiple stages at any time. The predicted state of these plots against actual state may also be shown, when a predictor is registered.

*Fig. 8: Four subplots of PlantViz showing actual and predicted values in various stages of SWaT*

### Registration for new ADM

As researchers continue to develop new ADMs, PlantViz allows the new ADMs to be registered and integrated.

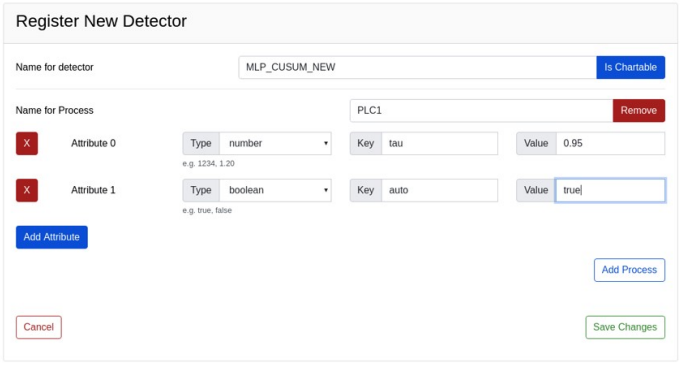


*Fig. 9: PlantViz allows new ADMs to be registered with run-time parameters being set by the user*

### Anomaly Alarm and Historical Anomalous Data

After an ADMs is registered, the same data is sent to it. If an anomaly is detected, a notification is triggered in the status bar to alert the user . A historical view of the anomalies detected is also available for analysis. Anomalies are grouped based on consecutive triggers. This grouping enables a user to analyse the anomalies based on uninterrupted and sequential triggers.

# Attack Tool for Validating Defence Mechanisms

**By Beebi Siti Salimah Binte Liyakkathali, Research Assistant**

Critical Information infrastructure refers to sectors that are important to provide services to a nation. Any loss or compromise of these essential services will have debilitating effect on a nation's ability to function properly. With the rise in the number and sophistication of cyber attacks, there also needs to be, at a minimum, a corresponding growth and innovation in defence mechanisms.

An attack suite was specially crafted to validate the effectiveness of a defence mechanism for CII, . This attack suite consists of A6-L0 and A6-L1. The A6-L0 attack tool, developed by Salimah, consists of component instrument-based attacks at Layer 0 of SWaT's network. In SWaT, Layer 0 is the communication between the Programmable Logic Controller (PLC) and the Remote Input Output

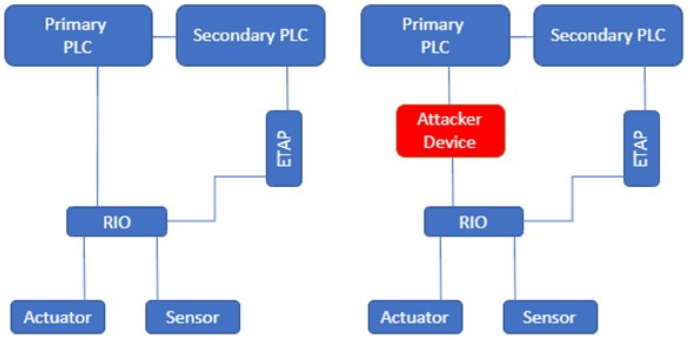


***Fig. 10: The network architecture at layer 0 of SWaT network (left) and how communications between the PLC and RIO can be manipulated (right, red box)***

(RIO) module. RIO module translates signals to bytes where each byte or bit corelates to input/output signals. The A6–L0 tool emulates a Man-In-the-Middle attack where communications between the RIO and PLC are manipulated (see Figure 10), resulting in abnormalities not being reflected on the plant's engineering workstation. An example of A6–L0's attack would be switching on the motorised valve (MV101) in Stage 1 to increase the volume of water in tank. This attack scenario is carried out by sending an "ON" signal of MV101 to the RIO while simultaneously sending an "OFF" signal of MV101 to the PLC. With this, the plant operator would still see that MV101 is switched off and not take corrective measures to prevent the tank from overflowing.

A mutation can be applied to attacks. One such example is that an invalid command (a value other than 1) can be input to switch on a pump (the valid commands for turning on and off the pump are 1 and 0 respectively).

The A6-L0 tool is an **aid to researchers in designing cyber attack experiments and using it to validate and strengthen defence mechanisms** developed within iTrust and those in the industry.

## Virtual and Mixed Reality for Security of Critical City-Scale Cyber-Physical Systems

**By Siddhant Shrivastava, Research Assistant**

VVateR is a virtual three-dimensional world for visualising Cyber-Physical Systems such as a city-wide water treatment and water distribution plant. A key novelty of VVateR is its ability to **enable visualisation of cyber- attacks, the resulting process anomalies, and whether or not the anomaly is detected.**

VVateR is currently operational in iTrust. It is connected to the SWaT and WADI testbeds. VVateR is accessed by wearing a virtual reality headset where the user/gamer can move about and interact with the plant in the virtual space. This opens up the plants for remote worldwide research collaboration and aids in capturing context from the plant that Mixed Reality promises to bring to industrial settings.

VVateR helps **visualise the interconnectedness of various infrastructures and the effects of cyber-physical attacks** through complex and dangerous scenarios that can be safely tested in a virtual setting. Observing slow historical plant operation and path of attacks at varying timelapse rates makes the process of reconnaissance and incident-analysis arguably faster and more visually engaging than an analysis of the database logs. By acting as a Digital Twin when connected to a simulator, one can come up with numerous attack/defense scenarios and serious gamified challenges for training purposes. All these factors increase the preparedness of operators, policymakers, governments, and other relevant stakeholders in strengthening their cities and Critical Infrastructures through security by design.

***Fig. 11: Chilean President Sebastián Piñera tries on the VVater***

The project has been presented to and commended by the President of Chile (Fig. 11), the US Navy Head of Research, PUB and NRF. From April to May 2019, it was presented at Department of Homeland Security's Industrial Control Systems Joint Working Group, Stanford University's Computer Systems Colloqium, Carne-

gie Mellon University's Institute of Software Engineering Seminar, New York University Tisch School of the Arts at Broadway, University of California Berkeley, and University of Missouri Kansas City. It was livestreamed and recorded on Stanford University's YouTube channel. The project won the 'Best Innovation Award' – a prize sponsored by Entrepreneur First at Research Fest in Jan 19. The team, led by Siddhant Shrivastava, consists of Prof. Aditya Mathur, and SUTD undergraduates Aiden Chia, Jason Chow, Ryan Gen, Monica Natalia, Marcel Prasetyo and Xiang Qian Ong.

## ASEAN ICT Awards 2018

Awards

**iTrust brings home the gold award for technology to secure ICS data**

Judges from the 10 ASEAN countries awarded SUTD the **Gold medal (Research and Development category)** at the ASEAN ICT Awards 2018 (AICTA) on 5 December. The win was for the technology "ICS:BlockOpS" developed by iTrust.

ICS:BlockOpS uses blockchain technology and redundancy capabilities to **ensure operational and network traffic data stored in an industrial control system (ICS) is secure and can be trusted.** By constantly validating the data integrity in the background, it is able to generate an alert when data has been tampered (modified or deleted), and enable its recovery. All these functions can be managed through a user-friendly graphical user interface. An advantage of the ICS:BlockOps technology is that it can be **easily integrated into existing ICS** and work alongside the historian without affecting its data flow.

The ICS:BlockOps technology is an end-to-end prototype which has been implemented the Secure Water Treatment (SWaT) testbed. A patent has also been filed for the technology.

"SUTD is young university and was established in 2012. This award is a recognition that we are moving in the right direction in our motto: **A Better World by Design.** We are trying to bring to market a technology that can help improve the safety and security of critical infrastructure, and this award will certainly help us in this regard," says Mark Goh, senior manager at iTrust who

***Fig. 12: Senior Minister of State for Communications and Information Dr Janil Puthucheary presenting the award to Mark Goh (centre) and Aung Maw (right), the student who developed ICS:BlockOps***

presented the technology and accepted the award on behalf of SUTD.

AICTA is a project that is in-line with one of the six Strategic Thrusts, Innovations as stated in the ASEAN ICT Masterplan (AIM) 2015 under the initiative 3.2 'Promote Innovation and collaborations amongst government, businesses, citizens and other institution'. The awards aims to **recognise the best ICT achievement among entrepreneurs across the ASEAN region.**

## Best Research-Oriented Paper Award

A paper, "Deep-Learning Approach to the Detection and Localisation of Cyber-Physical Attacks on Water Distribution Systems," co-authored by **iTrust postdoc Dr Riccardo Taormina and Asst Prof Stefano Galelli** was selected by the Editor of the Journal of Water Resources Planning and Management to receive the 2019 Best Research-Oriented Paper Award. The award was presented to them at the World Environmental & Water Resources Congress in Pittsburgh, Pennsylvania on 21 May 19.

On 21 Sep 18 iTrust was awarded a **"High Recognition for Depth of Research on Industrial Cybersecurity"** by Kaspersky, a security company. Dr Riccardo Taormina received the award on behalf of iTrust at the Kaspersky Industrial Cybersecurity Conference in Sochi, Russia.

Feel free to reach out to us to explore research collaborations, testbed usage and training and testing services.

## Management

**Mr Ivan LEE**
Deputy Director, Cyber Security Technologies
*ivan_lee@sutd.edu.sg*

**Prof. Aditya P MATHUR**
iTrust Centre Director
Professor of Computer Science, Purdue University, USA
*aditya_mathur@sutd.edu.sg*

**Prof. Jianying ZHOU**
Professor & Co-Centre Director
*jianying_zhou@sutd.edu.sg*

## National Satellite of Excellence

**Ms Angie NG**
Deputy Manager
*angie_ng@sutd.edu.sg*

**Ms Priscilla PANG**
Manager
*priscilla_pang@sutd.edu.sg*

**General Enquiries**
*nsoe_destsci@sutd.edu.sg*

## iTrust Laboratories

**Dr AUNG Yan Lin**
Senior Engineer (IoT)
*linaung_yan@sutd.edu.sg*

**Ms Liqun DING**
Specialist (Power & Training Skids)
*ding_liqun@sutd.edu.sg*

**Mr Mark GOH**
Senior Manager
*mark_goh@sutd.edu.sg*

**Mr Desmond WAN**
Senior Technologist (Water)
*desmond_wan@sutd.edu.sg*

iTrust
Centre for Research in Cyber Security