An iTrust Newsletter

Jan – Mar | Issue 4

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

From Centre Director's Desk

Participants at the opening ceremony of SG-CRC 2016

Dear Reader:

Greetings and a very Happy New Year! Welcome to the fourth issue of iTrust Times.

Indeed, at iTrust the times are getting increasingly exciting. iTrust was given an opportunity to host the inaugural Singapore Cybersecurity R&D Conference (SG-CRC) 2016. And, we did it! Yes, the two day conference was a resounding success, with high quality invited talks and papers presented, and attracting over 250 attendees from Singapore and abroad. The baton has now been handed over to Prof Abhik Roychoudhary (NUS) who will chair SG-CRC 2017.

iTrust looks forward to its three new testbeds – Water Distribution (WADI), Electric Power and Intelligent Control (EPIC), and IoT – being operational in 2016. The existing SWaT testbed will be interconnected to WADI and EPIC to allow the study of cascading effects of cyber attacks; part of this work is being carried out in collaboration with Prof Chris Hankin and Dr Deeph Chana of Imperial College, London.

I am proud to mention that iTrust researchers have been successful in publishing their work related to the design of secure CPS in top international conferences. The published work includes novel attacker models, tools for attack simulation, and powerful attack detection methods. The testbeds are a key source of our strength and enable us to experimentally validate our research.

The international footprint of iTrust continues to expand. Our researchers are collaborating with those from MIT, UT Dallas, Ben Gurion, and Technion. Companies from across the globe – Check Point, ICS2, CYBERBIT and Deloitt– have reached out to iTrust to assess the effectiveness of commercially available security solutions using the SWaT testbed. More are likewise planning to do the same.

iTrust is a welcoming and friendly research centre. Let us know if you are interested in participating in this exciting journey towards highly resilient CPS.

Aditya Mathur
Professor and Head of Information Systems Technology and Design Pillar, and
Centre Director, iTrust

In This Issue

SG-CRC 2016

Singapore
Cybersecurity R&D Conference

Last May Ponemon Institute, a survey company, released a study in which 350 companies were interviewed. The survey found that the cost of data breach averaged US$3.8 million (S$5.3 million). A similar study done by PwC - an auditing firm - in the same year determined this cost to be £2.2 million (S$4.6 million) for large organisations. Can security by design reduce these unnecessary risks and costs?

Security by Design brings a technically grounded element of design that integrates cyber security into a system early in the process rather than an afterthought. This was the theme at the inaugural Singapore Cybersecurity R&D Conference (SG-CRC) 2016 that was held at the Singapore University of Technology and Design (SUTD) on 14 and 15 January 2016. Organised by iTrust, SUTD's Centre for Research in Cyber Security, the conference was supported under the National Cybersecurity R&D (NCR) Programme, with a host of participating government agencies: the National Research Foundation (NRF), Ministry of Defence (MINDEF), Ministry of Home Affairs (MHA), National Security Coordination Secretariat (NSCS), Infocomm Development Authority (IDA), Cyber Security Agency (CSA) and Economic Development Board (EDB). Given that it was the first conference held under the NCR Programme, the organisers were pleasantly surprised by the strong turnout of more than 250 participants from government agencies, industry and the academia.

At the opening ceremony at SUTD's Auditorium, SUTD President Prof Tom Magnanti thanked the participants for their support in his welcome address. In highlighting how cyber technologies have pervaded our everyday lives, he shared a personal experience in which fraudulent and unauthorised transactions in his credit card occurred not once, but twice, while he was overseas. It was also with such cyber threats in mind that testbeds are built, and being built, to ensure that SUTD's applied research have direct relevance to, and use by the industry. The conference Guest of Honour was the Chairman of the Agency for Science, Technology and Research (A*STAR) Mr Lim Chuan Poh, who delivered the opening remarks. In it, Mr Lim noted the parallel progress of Singapore as a Smart Nation and the proliferation of IoT technologies and devices, as well as the rise of cyber threats that inevitably tail along with the increased use of such technologies. Through the conference, he hoped that the cybersecurity community could foster and grow partnerships and spark off new research and business ideas.

SUTD President Prof Magnanti (left) and A*STAR Chairman Mr Lim (right) delivering the welcome address and opening remarks respectively

A total of 22 submissions were received in response to the call for papers. Each submission was reviewed by at least two members of an international programme committee. Based on the reviews, six papers were selected for research paper presentation under the "Regular Paper" category and seven in the "Short Paper" category. The papers are available for download at the following site:

http://ebooks.iospress.nl/volume/proceedings-of-the-singapore-cyber-security-conference-sg-crc-2016-cyber-security-by-design

Leading researchers in cybersecurity were invited to deliver a keynote address (Prof Dawn Song, UC Berkeley) and presentations (Prof David Basin, ETH Zurich; Dr Dimitrios Serpanos, QCRI). Prof Song's presentation "Next-Generation Security Technologies in a Connected and Intelligent World" gave an overview of the different approaches to security and described how new techniques from her recent projects - Secure by Construction and Secure by Learning - provide better security than traditional approaches.

On Day 2, Prof Basin described an approach to cyber security by design through his presentation on "Developing Security Protocols by Refinement". In this strategy, abstract security goals are transformed into protocols that are secure when operating over an insecure channel controlled by a Dolev-Yao-style intruder. For design at the industrial control systems level, Dr Serpanos proposed a behaviour-based approach which is both secure and resilient. His group's approach includes a novel method for vulnerability analysis of processes through the use of a middleware, ARMET, which detects, diagnoses, repairs and recovers a system under (a suspected) attack.

Left to right: Prof Dawn Song (UC Berkeley), Prof David Basin (ETH Zurich), Dr Dimitrios Serpanos (QCRI) delivering their keynotes

Interspersed among the presentations were project updates from the seven NCR Programme grant recipients, research paper presentations, industry insights into security, and a cyber crime panel discussion. The research paper presentations were grouped into Mobile and Internet Security; Cyber Physical Systems; and Cyber Forensics. The industry were invited to share insights into security in the course of their work. BlackBerry (Android security), Check Point Software Technologies (intrusion detection), Custodio (review of cybersecurity technologies), and Parasoft South East Asia (source code security) formed this engaging session.

At the Cyber Crime Panel Discussion, the rich diversity of panelists from law enforcement agencies (Dr Madan Oberoi, INTERPOL; SUPT Teo Wee Meng, Singapore Police Force), academia (Assoc Prof Adams Kong, NTU) and industry (Mr Vitaly Kamluk, Kaspersky Lab) ensured that cyber crime was discussed and approached with different lens. Questions fielded from the audience and moderated by Prof Abhik Roychoudhury brought about an informative discussion for the participants.

Cyber Crime Panel (from left to right): Dr Oberoi (INTERPOL), Mr Kamluk (Kaspersky Lab), Prof Roychoudhury (NUS; moderator), SUPT Teo (SPF), and Assoc Prof Kong (NTU)

Next year's SG-CRC will be organised by the National University of Singapore (NUS) as chair and Nanyang Technological University (NTU) as co-chair.

Events

Despite the holiday season, iTrust was involved in a flurry of activities from Nov 2015 to Feb 2016.

Ministerial visit

Minister Yaacob Ibrahim (second from left) being briefed on SUTD and iTrust

Minister for Communications and Information (MCI) and Minister-In-Charge of Cyber Security Dr Yaacob Ibrahim and the Chief Executive of Cyber Security Agency (CSA) Mr Daivd Koh led a delegation visit to iTrust on 8 December 2015. They were briefed on SUTD and iTrust, including our research focus and capabilities, facilities, and collaborations with government agencies, industry and academia. iTrust Centre Director Prof Aditya Mathur led a tour of the Secure Water Treatment (SWaT) testbed. Students William Koh, and Yong Ching Yan demonstrated their projects on cyber attack and defence mechanisms on the SWaT testbed, and Muhammad Hatib on the Cyber Patrol project. The visit was featured in The Straits Times and Berita Harian, the local Malay newspaper.

iTrust Seminar Series

On 25 November 2015, Asst Prof Yilin Mo, from the School of Electrical and Electronic Engineering at Nanyang Technological University, delivered a talk on **"Secure Information Fusion in Cyber-Physical Systems"**, in which he pointed out that despite the tight coupling between information and communication technologies and physical systems in CPS, there might exist limits in the communication which allow for an attack to go undetected.

Prof Abhik Roychoudhury, from the School of Computing at the National University of Singapore (NUS), was invited to deliver a talk on 27 November 2015. His talk - **SemFix and Beyond: Programme Repair via Semantic Analysis** - introduced and compared two automated program repair methods: search-based program repair and semantic analysis based repair.

Cybersecurity Workshops

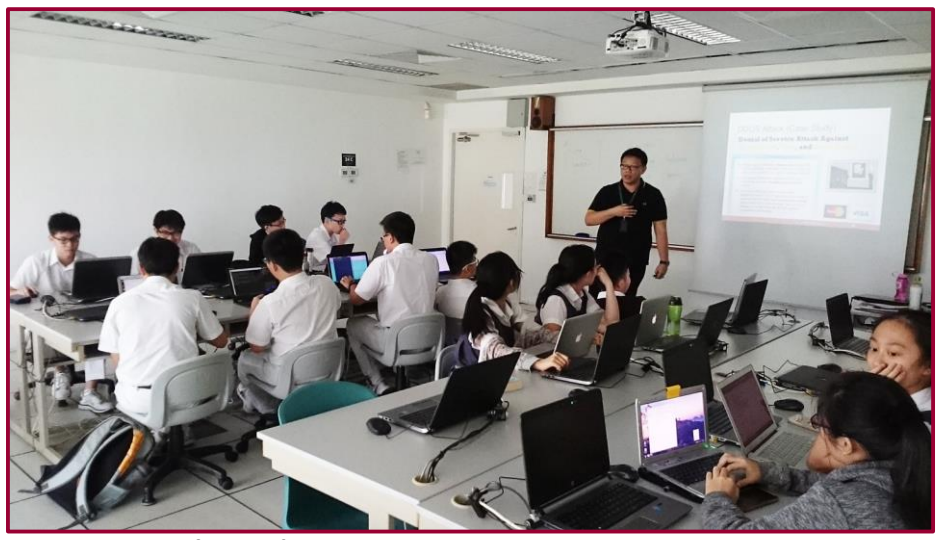
By Tan Yong Sheng

As part of its outreach activities and knowledge transfer to students, iTrust conducted a Cybersecurity Workshop during SUTD's Individual Activity Period (IAP), from 18 to 19 January 2016. The workshop covered topics such as Fundamental Networks, Introduction to Cyber Security, Introduction to Ethical Hacking and Advanced Hacking.

Workshop conductor Ivan Lee, iTrust's Senior Associate Director, sharing a light hearted moment with students at the workshop

To put their learning into practice, the students participated in a "Capture the Flag" game scenario created by iTrust, where they were tasked to perform a range of offensive and defensive strategies.

Beyond SUTD, a team of iTrust's technical staff were at Raffles Junior College (RJC) on 20 January 2016 to conduct two introductory workshops on Cybersecurity and Reverse Malware Engineering. The external workshop is part of iTrust's objective to increase awareness and interest in the field of cyber security among students. The workshops, attended by 26 students, received positive feedback.



Toh Jing Hui (SUTD) introducing cybersecurity concepts to RJC students

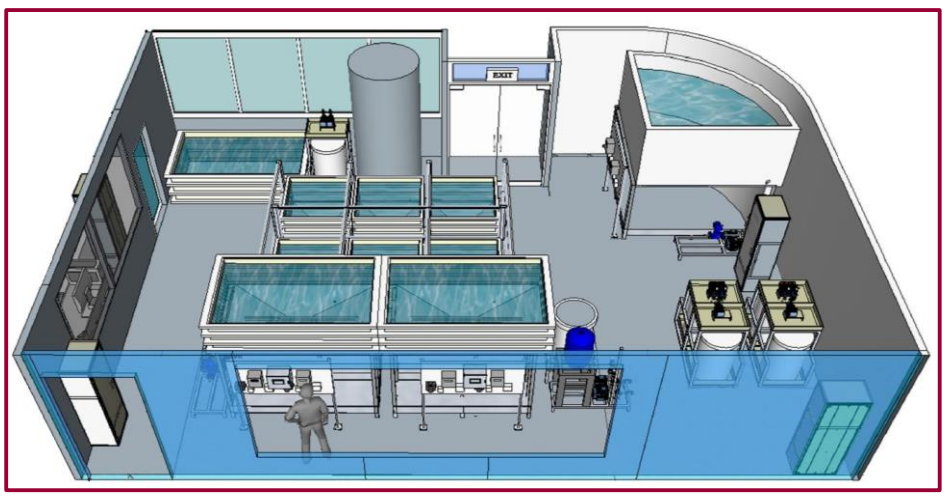
EY-SUTD OT Cyber Security Roundtable Discussion

Ernst and Young (E&Y), a professional services organisation, held a one-day EY-SUTD OT Cyber Security Conference on 3 February 2016, with support from iTrust. The forum, attended by about 150 people, was held at SUTD. It focused on critical infrastructure and the telecom and energy sector, and featured speakers from E&Y's global offices, as well as Assistant Professors from SUTD's Information Systems Technology and Design Pillar Martin Ochoa and Nils Tippenhauer.

New Testbeds

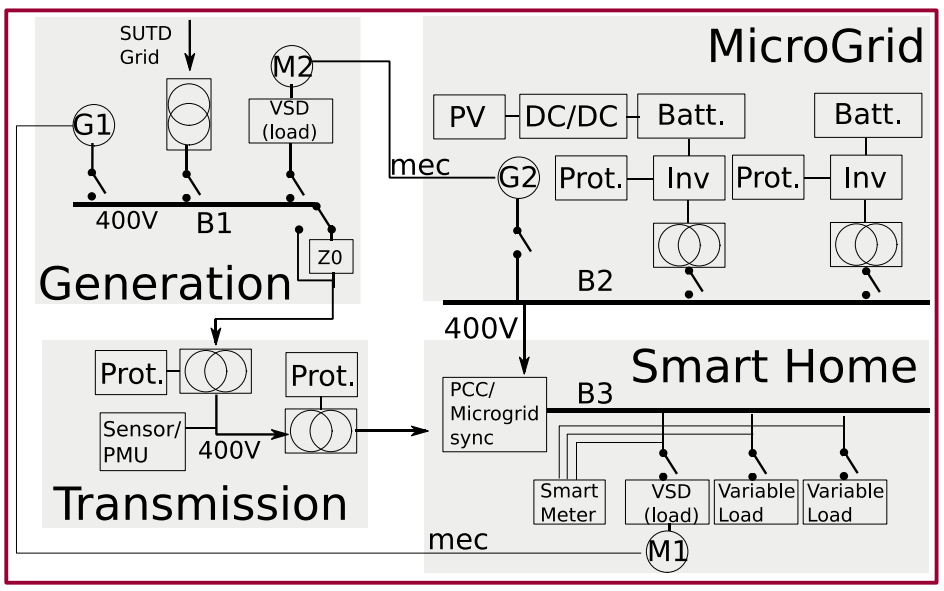
In Issue 1, we described iTrust as a host to a garden of testbeds. One such testbed – the Secure Water Treatment (SWaT) – is bearing fruit with multiple collaborations with industry (see following article). The other testbed – IoT lab – will be commissioned in March 2016. iTrust is also in the midst of constructing two new testbeds to enhance and expand our applied research into other CPS as well as IoT. These testbeds – Water Distribution (WADI), Electric Power and Intelligent Control (EPIC) – are expected to be operational in 2016, and will add to the diversity of research platforms available to researchers and collaborators, on top of the existing SWaT testbed.

WADI is a natural extension of SWaT, complete with storage tanks, chemical dosing systems, booster pumps and suitable valves, instrumentation and analysers. WADI will take in a portion of SWaT's reverse osmosis permeate and raw water, thus forming a complete and realistic water treatment, storage and distribution network. The combination of these two testbeds allow researchers to witness the cascading effects of cyber attacks on one testbed to another.



Draft layout diagram of WADI the testbed

The objective of EPIC is to support experimental investigation into the cyber security aspects of the distributed cyber components controlling the physical components such as generators and tap changing transformers. EPIC will comprise hardware components for electrical generation, transmission, loading and micro grid. Three ongoing research projects - Cyber Physical System Protection, Advancing Security of Public Infrastructure using Resilience and Economics, and the latter's water extension project – all contain research objectives and deliverables that can be supplemented and validated by the three testbeds described above. These include cyber attack and defence models, remote attestation, machine learning, economic models, trustworthy and secure data acquisition and communications in CPS etc.



Draft schematic diagram for the EPIC testbed

A fourth research project – Research & Security Innovation Lab for IoT – will benefit from the IoT lab. The lab, completed just last week, comprises IoT communication infrastructure, infrastructure to emulate specific environmental conditions for IoT devices and simulate attacks, and a suite of IoT devices. These equipment will allow researchers to test existing IoT prototypes and products for novel security vulnerabilities, and construct and validate experimentally their security prototypes and products. In the spirit of Security by Design, the IoT lab will allow researchers and designers at SUTD to incorporate security aspects into their design cycle at an early stage.

A Radio Frequency (RF) shielded room in the IoT laboratory

An RF shielded room within the IoT lab is also constructed to shield out stray electromagnetic interference to ensure accuracy of research results.

International Collaborations

Industry

By Jonathan Goh

In Nov and Dec 2015, iTrust welcomed two security companies – Check Point Software Technologies and CYBERBIT – to perform Proof of Concept (POC) on their respective intrusion detection solutions using the SWaT testbed.

Check Point SOFTWARE TECHNOLOGIES LTD.

ics² Intelligent Cyber Security for Industrial Control Systems

XIDS (Cross-platform Intrusion Detection System) is an advanced cybersecurity system co-developed by Check Point Software Technologies and ICS² (an

Israeli security firm) designed to take control on all events within a SCADA environment to prevent cyber-attacks on industrial control systems using multiple software security blades. The system monitors a plant's operation by looking for anomalies in the network communications payloads (Zero Day Attacks/BOTs) and in SCADA control data (process irregularities).

During the Initial Learning Phase, the team spent two weeks creating a baseline of the testbed's normal operations by learning its normal traffic and behaviour patterns. This learning process is based on a deep understanding of networking, industrial control processes and the laws that govern the underlying physical operations that they control. The XIDS also a second learning process by logging all SCADA networking communications, between the different components in the network. This enables the system to identify the communication patterns and create alerting policies.

In the Deployment Phase, XIDS was installed and activated in the SWaT testbed, and continuously monitored the SWaT plant's control data looking for and alerting any threats and behaviour anomalies such as irregular pump operations, abnormal pH readings, or incorrect water tank levels.

CYBERBIT
PROTECTING A NEW DIMENSION

CYBERBIT's POC goals were to demonstrate: (i) its AnD (Analysis and Detection) for SCADA's ability to monitor and analyse all transmissions and protocols, including CIP protocol; (ii) deep packet inspection and alerting of unauthorized network activity; and (iii) to provide analysis and network mapping capabilities.

CYBERBIT performed two levels of detection: detection in the plant network (level 1), and detection within the inner PLC network (level 0). At the plant network level, AnD for SCADA was able to detect the following anomalies: (i) addition of a new unauthorised device; (ii) illegal values sent to network components by an authorised device (insider threat); and legal values sent to network components by an unauthorised device. At the inner PLC network level, AnD for SCADA was able to identify a suspicious MAC address and in the process detect a man-in-the-middle attack that was executed on the network.

The POC experiments were supported by iTrust's researchers and laboratory engineer who helped to coordinate and perform a series of cyber-attacks on the testbeds.

Academia

UT Dallas

Jairo Giraldo and David Urbina, both postdocs from UT Dallas, arrived in Sep 2015 for a 3-month stint, as visiting researchers for the project "Advancing Security of Public Infrastructure using Resilience and Economics".

Jairo's work involved creating mathematical models of SWaT using CUSUM (cumulative sum, which is typically used for monitoring change detection). Having an estimated model of the plant would then allow researchers to design detection mechanisms that compare the current states of the system with its estimation, thereby detecting abnormal behaviours in the system. David, on the other hand, was tasked with creating different attacking scenarios/scripts in different network layers of SWaT system. The scripts are now being adopted by iTrust researchers to perform level 0 network attacks on SWaT.

MIT

A month before Eunsuk Kang arrived at iTrust, he was collaborating with iTrust's researcher Sridhar Adepu on applying formal methods to ICS. Together, they planned on how to implement the models on SWaT using Alloy. During his one week here he analysed the system for different types of attacks, while also automatically generating different attacks under various scenarios. Eunsuk and Sridhar continues to work closely to apply formal language to propose a security by design approach for CPS.

Visiting researchers to iTrust (from left to right): Jairo Giraldo, David Urbina (both UT Dallas), Eunsek Kang (MIT)

Visits to iTrust and SWaT testbed

Over the past few months, iTrust hosted visits from local and overseas guests ranging from academia, industry to government agencies:

- GIC (23 Dec 15)
- Delegates from the Global Young Scientists Summit 2016 (21 Jan 16)
- Delegates from EmTech Asia Conference 2016 (28 Jan 16)
  - Major General Thomas Masiello and Chief Scientist Dr. Azar Ali; U.S. Air Force (17 Feb 16)

In addition, **Channel NewsAsia**, a local news station, and **OpenGovAsia**, an online news platform, conducted interviews to feature iTrust and the SWaT testbed. Cyber security was also featured as a key thrust for a strong and smart nation in this year's **Total Defence Day** on 15 Feb 16. These articles can be accessed at iTrust's website at http://itrust.sutd.edu.sg/.

Profiles

Costas Courcoubetis

Prof. Costas A Courcoubetis was born in Athens, Greece. He received his Diploma (1977) from the National Technical University of Athens, Greece, in Electrical and Mechanical Engineering, his M.Sc. (1980) and Ph.D (1982) from the University of California, Berkeley, in Electrical Engineering and Computer Science.

From 1982 until 1990 he was Member of the Technical Staff (MTS) in the Mathematical Sciences Research Center, Bell Laboratories, Murray Hill, NJ, and from 1990 until 1999 he was Professor in the Computer Science Department at the University of Crete in Heraklion, Greece, and headed the Telecommunications and Networks Group at the Institute of Computer Science, FORTH. Since 2013 he is a Professor in both Engineering Systems and Design (ESD) and ISTD Pillars at SUTD. Costas' current research interests are economics and performance analysis of networks and internet technologies with applications in the development of pricing schemes that reduce congestion and enhance stability and robustness, regulation policy, smart grids and energy systems, resource sharing and auctions.

Besides leading a large number of research projects in these areas he has also published over 100 papers in scientific journals such as Operations Research, Mathematics of Operations Research, Journal on Applied Probability, ToN, IEEE Transactions in Communications, IEEE JSAC, SIAM Journal on Computing, etc. and in conferences such as FOCS, STOC, LICS, INFOCOM. GLOBCOM, ITC, ACM SIGMETRICS. Costas' work has over 12,000 citations according to the Google Scholar. He is co-author with Richard Weber of "Pricing Communication Networks: Economics, Technology and Modelling" (Wiley, 2003).

Stefano Galelli

Dr. Stefano Galelli graduated in Environmental and Land Planning Engineering at Politecnico di Milano in 2007, and he received a Ph.D. in Information and Communication Technology from the same university in early 2011.

Before joining SUTD as Assistant Professor, Stefano spent two years as Post-Doctoral Research Fellow at the Singapore-Delft Water Alliance (National University of Singapore), where he led the Hydro-informatics group. He was visiting scholar at MIT (US), Deltares (NL) and University of Western Australia. Dr. Galelli's research focuses on modelling and control of large-scale water resources systems, including aspects related to their cyber security.

Stefano is a member of the IFAC Technical Committee TC8.3 on Modelling and Control of Environmental Systems and of Environmental Modelling & Software editorial board. He also serves as Associate Editor for the Journal of Water Resources Planning and Management.

He received the Environmental Modelling & Software 2011 Outstanding Reviewer Award and an Early

Career Research Excellence Award (2014) by the international Environmental Modelling & Software society. He actively collaborates with several universities and research institutes, including MIT (US), Technion (IL), Politecnico di Milano (IT), TU Delft (NL), Deltares (NL), NUS, University of Western Australia and University of Adelaide.

Kandasamy Muruganandam

Kanda joined iTrust on 4 Jan 2016 as an IoT laboratory engineer. He graduated with a Masters of Computer Application from Anna University. Before joining iTrust, he worked at various MNC including Computer Science Corporation, Accenture and Cognizant. His roles there ranged from Lead Developer to Senior Developer. Kanda helped developed products and services for a spectrum of key industries, from telecommunications (Huawei), medical (Roche) to finance (PayPal). His job scope included requirement identification, design, coding, testing and resource allocation. Kanda has experience in software development using both Agile and Waterfall methodologies. In his leisure time, he loves spending time with his family, watching movies, exploring different places, culture and good food.

Muhamed Zhaffi Bin Mohamed Ibrahim

Zhaffi joined iTrust on 4 Jan 2016 as the laboratory engineer for EPIC testbed. He holds a Diploma in Electrical and Computer Control Engineering and Advanced Diploma in Power Systems Engineering from Singapore Polytechnic. He is a certified explosion proof inspector from Compex Singapore, and has completed industrial PLC programming from FESTO Singapore and Siemens Basic and Advanced PLC. Zhaffi has seven years of controls and instrumentation experience in the marine and oil and gas industry. Prior to joining iTrust, he worked in several MNCs including Keppel Offshore and Marine, National Oilwell Varco, and KCADeutag. In his free time, Zhaffi conducts research on PV implementation.

iTrust Staff

Mr Kaung Myat AUNG, *Laboratory Engineer (Water)*
kaungmyat_aung@sutd.edu.sg

Prof. Yuval ELOVICI, *Research Director*
yuval_elovici@sutd.edu.sg

Dr Jonathan GOH, *Research Scientist*
jonathan_goh@sutd.edu.sg

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

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

Prof. Aditya P MATHUR, *Professor & Head of Pillar, ISTD Pillar, SUTD Centre Director*
aditya_mathur@sutd.edu.sg

MUHAMED Zhaffi Bin Mohamed Ibrahim, *Laboratory Engineer (Power)*
zhaffi_ibrahim@sutd.edu.sg

Kandasamy MURUGANANDAM, *Laboratory Engineer (IoT)* Kandasamy_m@sutd.edu.sg

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

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

Mr TAN Yong Sheng, *Technical Officer*
yongsheng_tan@sutd.edu.sg

iTrust
Center for Research in Cyber Security
itrust.sutd.edu.sg