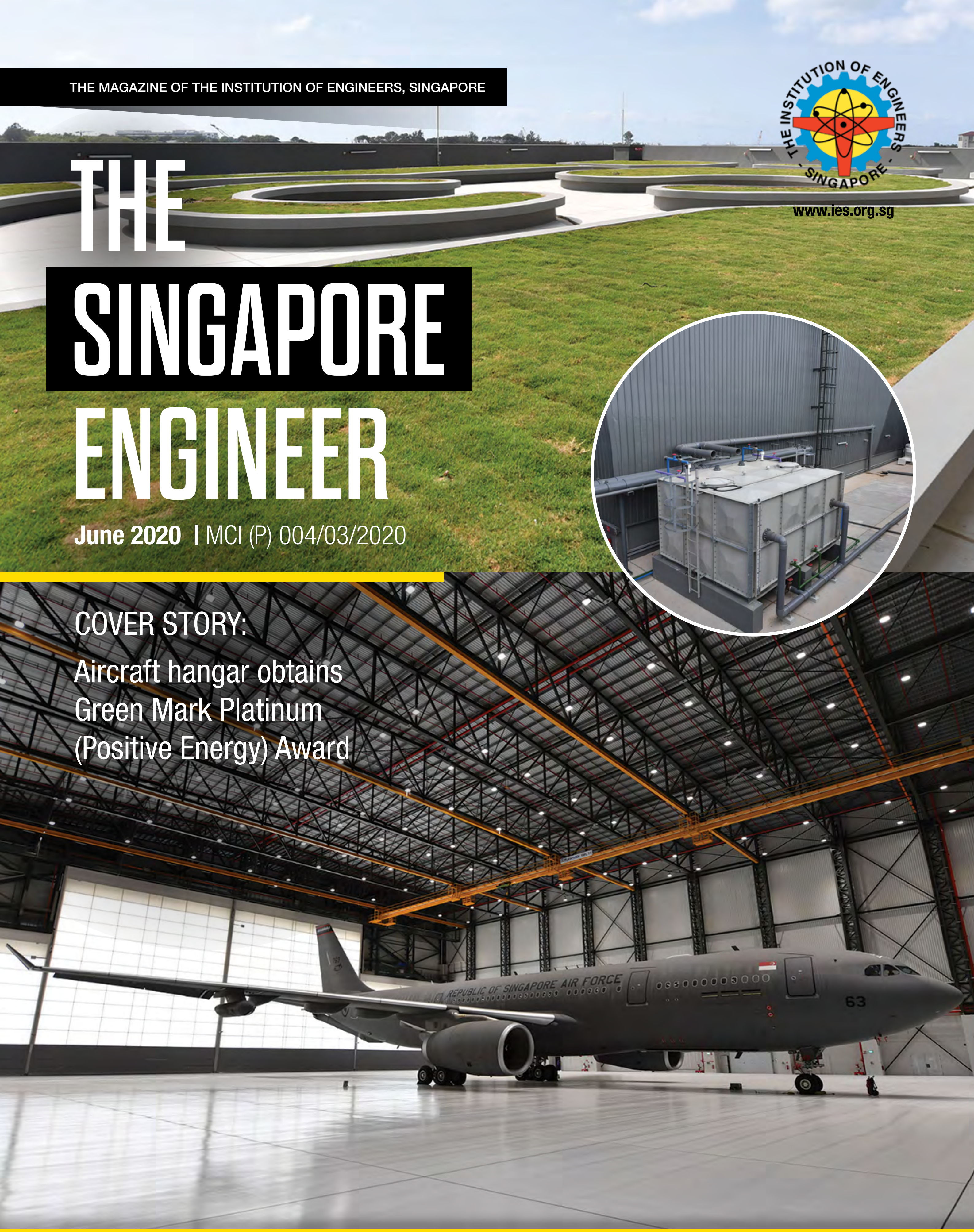
THE MAGAZINE OF THE INSTITUTION OF ENGINEERS, SINGAPORE

www.ies.org.sg

THE SINGAPORE ENGINEER

June 2020 I MCI (P) 004/03/2020



COVER STORY:

Aircraft hangar obtains Green Mark Platinum (Positive Energy) Award

PLUS

MEP ENGINEERING: Towards zero resubmissions

SMART CITIES: COVID-19 pandemic highlights the need for smarter and more adaptable cities

DIGITALISATION: The sprawling reach of complex threats

Marine & Offshore

Railway & Transport

Infrastructure

Energy

Chemical & Process

Aerospace

Environmental & Water

Systems

CONTENTS

FEATURES

President
Prof Yeoh Lean Weng

Chief Editor
T Bhaskaran
t_b_n8@yahoo.com

Publications Manager
Desmond Teo
desmond@iesnet.org.sg

Publications Executive
Queek Jiayu
jiayu@iesnet.org.sg

Editorial Panel
Dr Chandra Segaran
Prof Simon Yu
Dr Ang Keng Been
Mr Gary Chiam
Dr Victor Sim
Mr Syafiq Shahul
Dr Alexander Wiegand

Media Representative
Multimedia Communications (2000) Pte Ltd
sales@multimediacomms.sg

Design & layout by **2EZ Asia Pte Ltd**

Cover designed by **Irin Kuah**

Cover images by **MINDEF**

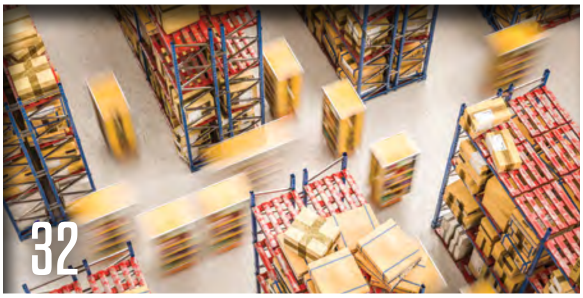
Published by
The Institution of Engineers, Singapore
70 Bukit Tinggi Road, Singapore 289758
Tel: 6469 5000 I Fax: 6467 1108

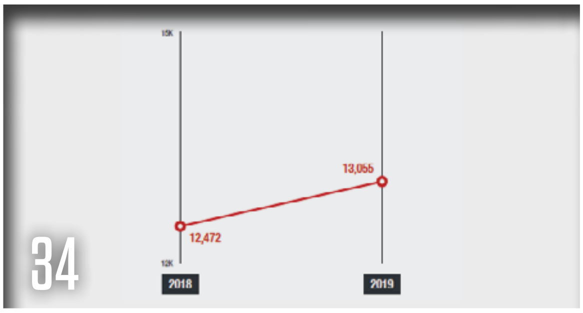
Printed in **Singapore**

www.ies.org.sg

SMART CITIES

DIGITALISATION





REGULAR SECTIONS

The Singapore Engineer is published monthly by The Institution of Engineers, Singapore (IES). The publication is distributed free-of-charge to IES members and affiliates. Views expressed in this publication do not necessarily reflect those of the Editor or IES. All rights reserved. No part of this magazine shall be reproduced, mechanically or electronically, without the prior consent of IES. Whilst every care is taken to ensure accuracy of the content at press time, IES will not be liable for any discrepancies. Unsolicited contributions are welcome but their inclusion in the magazine is at the discretion of the Editor.

SURBANA JURONG SIGNS GLOBAL COMMITMENT

TOWARDS MAKING ALL BUILDINGS NET ZERO CARBON BY 2050

Marking World Environment Day on 5 June 2020, Surbana Jurong, one of the largest Asia-based urban, infrastructure and management services consulting firms, announced that it has signed the World Green Building Council (WorldGBC) Net Zero Carbon Buildings Commitment.

The commitment challenges companies, cities, states and regions to reach net zero operating emissions in their global portfolios by 2030, and to advocate for all buildings to be net zero carbon by 2050. A net zero carbon building is a building that is highly energy-efficient and fully powered from on-site and/ or off-site renewable energy sources.

Surbana Jurong is one of 96 global businesses, cities and states which have signed the commitment. The commitment from businesses which are part of this net zero movement will reduce more than 3.3 million tonnes of carbon emissions collectively.

To act on its commitment to catalyse change, Surbana Jurong will develop and implement a carbon decarbonisation roadmap outlining key actions and milestones to achieve net zero carbon by 2030, and embark on sustainability reporting to demonstrate enhanced energy performance, reduced carbon emissions and progress towards net zero carbon.

Surbana Jurong will also continue to lead and advocate the transition towards net zero carbon buildings through its sustainability and multidisciplinary consultancy services, and test-bedding of innovative technologies. It has worked on net zero energy buildings such as the NUS School of Design and Environment 4, designed by SJ Architecture, and the Mohawk College Joyce Centre for Partnership & Innovation, in Hamilton, Ontario, Canada, designed by B+H, a member of Surbana Jurong Group.

Mr Wong Heang Fine, Group Chief Executive Officer of Surbana Jurong said, "We are taking accretive steps towards decarbonising the buildings and structures that we design for clients as well as those we use for our own operations. As a multidisciplinary urbanisation, infrastructure and managed services consultancy, Surbana Jurong is able to provide step change solutions for sustainability at every phase of a project lifecycle. Taken together as part of an integrated design, these solutions are aimed at accelerating the wide adoption of sustainability practices, affordably and effectively".

Advancing Net Zero

Advancing Net Zero is a global project by the World Green Building Council, aimed at accelerating uptake of net zero carbon buildings to 100% by 2050. The project works with members of the global Green Building Council network to develop tools and resources, including net zero carbon building certification schemes and training programmes, to support their advocacy work with their members and local governments, and build industry capacity.

Net zero energy building: NUS School of Design and Environment 4, designed by SJ Architecture. Image: Office of Estate Development, National University of Singapore.

Net zero energy building: Mohawk College Joyce Centre for Partnership & Innovation, in Hamilton, Ontario, Canada, designed by B+H, a member of Surbana Jurong Group.

SCHNEIDER ELECTRIC

AND AVEVA EXTEND PARTNERSHIP

Schneider Electric, a leader in digital transformation of energy management and automation, and AVEVA, a global leader in engineering and industrial software, recently announced their expanded partnership to deliver innovative solutions for the data centre market.

The combination of Schneider Electric's EcoStruxure Data Center Solutions with AVEVA Unified Operations Center, gives both deep and expansive visibility to day-to-day operations.

Schneider Electric's EcoStruxure Data Center Solutions bring together power, cooling, racks, and management systems to support deployment of IT equipment in all environments from small Edge applications to large Cloud data centres.

AVEVA's Unified Operations Center helps customers capitalise on digital technologies to transform their business by integrating and visualising all available data in context, be it operations, process, engineering, maintenance and financial data.

The new joint solutions provide a homogenous view of engineering, operations, and performance across a heterogenous, legacy installed base. Hyperscale data centre providers will benefit from this partnership by connecting platforms and data sets that previously existed in disparate systems. They will also be able to scale, regardless of the number of sites or global location. Data centre staff will be empowered to make faster, more informed decisions and optimise asset and operational efficiency throughout the data centre lifecycle. As a result, data centre providers can deliver a globally consistent experience to address the expanding digital infrastructure needs of their clients.

"At a time when the world's digital infrastructure is being pushed to its limits, Schneider and AVEVA are delivering a comprehensive solution for hyperscale data centres to operate and maintain their critical environments. The solution can take data that has long been managed at individual data centres, often in siloed sub-systems, normalise it across multiple sites and ultimately inform and provide enterprise level IT/OT/IoT integration to deliver real-time decision-making. The complete solution will deliver operational efficiency and a more reliable data centre fleet", said Pankaj Sharma, Executive Vice President of the Secure Power Division at Schneider Electric.

"AVEVA and Schneider Electric's unique partnership is already delivering tremendous value for our industrial customers across the board. It is a major strategic milestone for us to extend the partnership into new markets and reach more clients, combining AVEVA's strong heritage of delivering end-to-end unified solutions with Schneider Electric's deep data centre expertise and global execution capabilities. Our joint customers are empowered by the standardised systems and processes resulting in improved workforce efficiency across multiple sites and the entire enterprise", said Craig Hayman, CEO, AVEVA.

CDL wins multiple accolades at 5th Asia Sustainability Reporting Awards

City Developments Limited (CDL) emerged as the only Singapore company to win multiple accolades at the 5th Asia Sustainability Reporting Awards (ASRA), bringing home a total of three golds and one silver at the awards ceremony on 29 April 2020, hosted virtually due to the COVID-19 pandemic. CDL clinched gold for Asia's Best Integrated Report Award, the most prestigious award for sustainability reporting across the region, as well as gold for Best Carbon Disclosure, and Best Sustainability Report (Digital), and a silver for Best Sustainability Report (Design).

CDL has been an early adopter and pioneer of sustainability reporting and was the first corporation in Singapore to publish a dedicated sustainability report using the Global Reporting Initiative (GRI) framework since 2008. Since then, it has continued to refine metrics and raise targets that are used to assess and manage climate-related risks and opportunities which are material to CDL's business. Last year, CDL played a key role in spearheading the establishment of the GRI Regional Hub in Singapore and continues to support the GRI's mission to raise the standards of sustainability reporting and disclosure in Singapore and the region.

Ms Esther An, CDL Chief Sustainability Officer, in her acceptance speech at the virtual awards presentation, said, "CDL is truly honoured to be recognised for its sustainability reporting efforts and conferred with Asia's Best Integrated Report Award, one of the top accolades presented at the awards ceremony. Sustainability reporting has provided us with good guidance on the strategic integration of material ESG issues, target-setting and tracking, stakeholder engagement and effective communication to a global audience".

ASRA 2019 saw 80 shortlisted companies from 13 countries competing in the finals across 19 award categories. The winners were selected from 461 entries received from 16 countries in Asia.

POWER PURCHASE AGREEMENT SIGNED TO BUILD FLOATING SOLAR SYSTEM

Singapore's National Water Agency PUB, and Sembcorp Floating Solar Singapore, a wholly-owned subsidiary of Sembcorp Industries (Sembcorp), have signed a 25-year power purchase agreement (PPA) to build a 60 megawatt-peak (MWp) floating solar photovoltaic (PV) system on Tengeh Reservoir. The signing of the agreement followed PUB's announcement in February this year, that it has appointed Sembcorp to design, build, own and operate this project.

When fully operational in 2021, this project aims to be a global showcase of operational excellence and safety as Singapore's largest, as well as one of the world's largest, inland floating solar PV systems. The solar power generated will meet the day-to-day energy needs for operations at PUB's five local waterworks, including Marina Barrage. This makes Singapore one of the few countries in the world to achieve 100% green waterworks, when the project is completed.

Under the agreement, Sembcorp Floating Solar Singapore will deploy over 146,000 solar panels at Tengeh Reservoir in Tuas, covering an area of around 45 football fields. At 60 MWp, the floating solar PV system will generate enough energy to power about 16,000 four-room HDB flats for a year and offset about 32 kilotonnes of carbon emissions annually.

Utilising highly efficient PV modules that maximise solar energy yield, the panels would be installed on corrosion-resistant floats that are certified to be of food-grade quality. Prior to deployment, extensive studies have been conducted to ensure that the PV modules pose minimal impact to the environment and water quality.

Mr Ng Joo Hee, Chief Executive, PUB, said, "With this floating solar power plant, which we believe to be one of the largest in the world, PUB takes a big step towards enduring energy sustainability in water treatment. Solar energy is plentiful, clean and green, and is key to reducing PUB's and also Singapore's carbon footprint".

Mr Neil McGregor, Group President & CEO, Sembcorp Industries, said, "Sembcorp is privileged to partner PUB in their ongoing sustainability journey, greening their waterworks as well as producing more solar power in Singapore's total electricity mix. As we continue to reshape our portfolio towards renewables, we are excited to apply our proven capabilities and innovations in this field on this landmark project. When complete, the Tengeh floating solar installation will not only represent a world-class engineering feat but also help to support Singapore's solar target of 2 gigawatt-peak (GWp) by 2030".

PUB's floating test-bed on Tengeh Reservoir. Images: PUB, Singapore's National Water Agency.

NEW BATTERY PERFORMANCE

STANDARD PROPOSED TO STANDARDS AUSTRALIA

DNV GL, a global quality assurance and risk management company, recently announced the completion of the Australian Battery Performance Standard (ABPS) project which started development in 2018.

A draft standard, addressing which energy storage system is best suited to residential and small-scale commercial applications, has been submitted by DNV GL on behalf of the ABPS project consortium comprising leading Australian energy organisations, the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Deakin University and the Smart Energy Council.

According to the Department of Industry, Science, Energy and Resources, Australia has the highest uptake of solar globally, with 2.37 million or 21% of all homes with rooftop photovoltaics (PV) systems installed. Installation of domestic battery storage is currently being held back, in part, by the difficulty end-customers face in choosing the right battery system for their needs.

To address this, the draft standard specifies key performance metrics for manufacturers to report on in a consistent way, which will make it easier for consumers to compare battery energy storage systems. The metrics will include properties such as maximum and sustained power, capacity and efficiency, which are all typical metrics in battery testing, but not always reported by battery system manufacturers or measured in the same manner. Test protocols have been designed specifically to provide battery performance data relevant to Australian climatic conditions and solar PV production patterns.

This draft standard was submitted to Standards Australia after a comprehensive two-year development process which received AUD 1.44 million in funding from the Australian Renewable Energy Agency (ARENA) through its Advancing Renewables Program, and the Victorian Government through its New Energy Jobs Fund.

ARENA CEO Darren Miller said, "Energy storage is shaping up to be an important feature of our rapidly evolving energy system. As rooftop solar penetration continues to increase, and more people look to store their solar energy during the day and minimise what they consume from the grid in the evening, it is important that consumers are informed about how well batteries perform over their lifetime, to aid their investment decision".

Nicolas Renon, Executive Vice President Asia Pacific Region, at DNV GL - Energy said, "This standard will help address the consumers' dilemma in choosing the energy storage system best suited to their needs, and empower them to play their part in moving towards a cleaner future".

To support the draft standard, the project consortium will be releasing an interim best practice guide, which can be used until such time as the standard is adopted. This will include a step-by-step description of how to carry out the necessary testing, along with background information on how to confirm with the best practice guide until the standard is made official by Standards Australia.

The consortium also discovered that no performance standard for batteries connected to domestic/small commercial solar PV exists anywhere in the world, so this standard has the potential to become a new global standard once in effect.

The need for a sustainable recovery from COVID-19

International investor groups, including the Investor Group on Climate Change (IGCC), have encouraged global governments to ensure they are planning for a sustainable recovery from the COVID-19 pandemic by factoring in climate change risk into economic recovery plans.

A global statement, which has been sent to G20 countries and New Zealand, reinforces the principle that governments' first priority amid the COVID-19 pandemic is to save lives and provide financial relief to support the most vulnerable.

As governments look to spark longer-term economic recovery, the investor groups warn locking in carbon-intensive economic activities will only exacerbate systemic climate risk and expose economies to escalating shocks. The groups say governments should instead look to drive efficient private capital investment that can create fresh employment and economic growth, by prioritising net zero emissions projects in areas like infrastructure, transport, property and energy.

The global statement is signed by the heads of the founding partner organisations of The Investor Agenda, including IGCC, the Asia Investor Group on Climate Change, the Institutional Investor Group on Climate Change, Ceres, Principles for Responsible Investment, CDP and the United Nations Environment Programme Finance Initiative.

The investor organisations recommend governments adopt the following measures:

- Prioritise human relief and job creation.
- Uphold the Paris Agreement.
- Ensure corporate assistance assesses climate risk.
- Prioritise climate resiliency and net zero emissions solutions.
- Embed investor participation in recovery planning.

SUEZ NWS AMONG CHINA'S MOST INFLUENTIAL WATER COMPANIES

SUEZ NWS came in fourth place in the 2019 Top Ten Most Influential Water Companies in China rankings. The accolade sees SUEZ NWS becoming the only foreign company to have achieved the prestigious ranking for 17 consecutive years since the list's inception.

The Top 10 Most Influential Water Companies in China Award is organised by the E20 Environment Platform which rates water companies on the basis of selection criteria that include the total and incremental capacity of projects they fund and operate, dynamic market influence, integrated service capabilities, market position, activeness, strategic core competitiveness, involvement in charitable causes, brand reputation and influence.

Having established a foothold in China, some 40 years ago and grown its busiiness over the years, SUEZ has prioritised its future business development in three areas:

- Waste sector: Hazardous waste management is a key area. Currently, SUEZ has built and operated nine hazardous waste treatment plants in mainland China.
- Industrial sector: The water sector in China still presents significant growth potential for the company which will be able to leverage synergies from the GE Water acquisition.
- Smart solutions: For conventional municipal water services, smart water solutions will become the new growth engine. To deliver more smart solutions to customers, SUEZ will increase its investments in R&D, innovation, and digitisation by 50%, by 2023.

APPLICATION OF INJECTION MOULDING

ENABLES PRODUCTION OF FACE SHIELDS

At the moment, protection from Covid-19 is one of the world's most important challenges. However, a sufficient amount of appropriate equipment of the necessary quality is not quickly available on the market. Solutions include face shields which private persons and companies are currently making all over the world using 3D printing.

German company, igus GmbH, a leading global manufacturer of energy chain systems and polymer plain bearings, has now speeded up the production with injection moulding. The motion plastics specialist is donating 200,000 complete face shields to German schools, as well as firefighters, elderly care institutions and medical practices. Face shields can be a part of a security concept, in addition to social distancing and disinfectants.

In order to protect doctors, nursing personnel and other people who work directly with patients, Prusa, a 3D printer manufacturer, has developed a face shield and placed the design on the Internet for downloading, free-of-charge. The aim is to produce the face shields on as many 3D printers as possible. The project is already regarded as a success, in that individuals, manufacturer networks and companies all over the world are participating in the scheme and are working flat out to additively produce the face shields.

Further, initiatives such as 'Operation Shields Up!' in the US are bringing volunteers together on their platforms. igus GmbH is taking part in this worldwide collaborative project and is making use of the advantages of injection moulding.

Using injection moulding, igus GmbH, from Cologne, Germany, is producing and donating face shields to the city. Image: igus GmbH.

Cost-effective production of face shields

Early on, 3D printing companies had asked igus whether it could provide them with material. But that would not have solved the real problem which is that if a 3D printer is used, production of the headband is expensive and takes more than two hours. This means that only a few parts can be made per day. Accordingly, igus decided to rely on the advantages of another method, namely, injection moulding. The company produced the right tool within six days, instead of the usual six weeks, thereby enabling the production of two headbands per minute. The face shields are supplied by igus as a kit, including assembly instructions, directly to the schools in Germany.

Grundfos proceeds to acquire Eurowater

Grundfos recently entered into an agreement to acquire Eurowater, thereby significantly strengthening its ongoing efforts to pioneer solutions to tackle global water challenges.

The acquisition aligns closely with Grundfos' strategy to strengthen its innovation leadership within water technology, and supports the company's purpose to pioneer solutions to the world's water and climate challenges and improve the quality of life for people.

"Eurowater brings a broad portfolio of solutions and a deep understanding of water treatment applications and end-users. This will enable us to strengthen our value proposition to customers. When complete, this acquisition will further advance us in our important work to address water challenges on a global scale", said Ulrik Gernow, Group Executive Vice President, CMO, at Grundfos.

The Eurowater and Grundfos businesses share many similarities, including a sharp focus on innovation and the delivery of high quality products and value-added services to customers. Culturally, the two organisations match well, both being purpose-driven and customer-centric.

"We took over the company 17 years ago from the Scherfig family which has owned the company since its foundation in 1936. With the global reach and presence of Grundfos and our extensive experience in producing first class products, we see great opportunities to boost the development of innovative and water-efficient solutions to the benefit of our many customers", said Torben Buhl, Managing Director of Eurowater.

Headquartered in Denmark, Eurowater serves primarily the European markets, with a range of water treatment offerings serving customers in the industrial and municipal sectors.

Grundfos is a global leader in advanced pump solutions and an innovator in water technology.

THEME FOR SIEW 2020 LAUNCHED

SIEW 2020
SINGAPORE INTERNATIONAL ENERGY WEEK

ENERGY MARKET AUTHORITY
Smart Energy, Sustainable Future

Despite a temporary drop in emissions caused by COVID-19, the urgent need to combat climate change remains. Against this backdrop, the Energy Market Authority (EMA), organisers of the Singapore International Energy Week (SIEW), recently presented 'Creating Our Low Carbon Energy Future Together' as the theme for SIEW 2020.

On the SIEW 2020 theme, Dr Koh Poh Koon, Senior Minister of State for the Ministry of Trade and Industry, said, "The theme highlights how governments and industries are faced with the urgent challenge of growing the economy in a sustainable manner. The uncertain global economic outlook would present even more challenges for the energy sector. I look forward to the meaningful discussions at SIEW on how we can create a low carbon energy future together".

EMA announced the theme at the inaugural SIEW 2020 Global Launch webinar. Speakers at the launch included Mr Neil Atkinson, Head of Oil Industry & Markets Division, International Energy Agency (IEA), and Mr Tan Cheng Guan, Head of Renewables & Environment, Sembcorp Industries. Moderating the discussion was Ms Goh Swee Chen, President, Global Compact Network Singapore.

Highlights at SIEW 2020

The Singapore Energy Summit will see a high-level panel comprising ministers and industry leaders delving deeper into the theme. The programme includes discussions on the pathways to our low carbon energy transition, the impact on the economy, and how we can tap into low carbon alternatives.

For the first time, Singapore and the IEA will co-host the 2nd Global Ministerial Conference on System Integration of Renewable Energy at SIEW.

Dr Fatih Birol, IEA's Executive Director, said, "The integration of variable renewable energy is a key part of strengthening modern, sustainable, and affordable energy systems. I am very pleased that the IEA will co-host the 2020 IEA System Integration of Renewable Energy Ministerial Meeting with the Government of Singapore at Southeast Asia's premier energy sector event, SIEW".

"This year, during the IEA's year of Clean Energy Transitions, we will bring together ministers and business leaders to discuss real world solutions and the latest developments to integrate growing shares of renewables - a critical part of the effort to enhance energy security, sustainability and affordability. Now, more than ever, governments and energy sector actors should prioritise the security of energy systems and this important event is designed to assist with this imperative", Dr Birol added.

S&P Global Platts will host a new conference on LNG & Hydrogen Gas Markets in Asia, with a special focus on the growth and development of hydrogen in the region.

Returning partner event, Asia Clean Energy Summit, will examine clean energy alternatives including floating solar photovoltaics. Asian Downstream Summit 2020 will be co-located with the Asian Refining Technology Conference, with a focus on sustainability & productivity in refining & petrochemicals.

Delegates can also look forward to report launches at the SIEW Energy Insights and SIEW Thinktank Roundtables. Returning roundtable hosts include Agora Energiewende; Energy Research Institute @ NTU (ERI@N); the Energy Studies Institute (ESI); and Institute of Energy Economics, Japan (IEEJ).

SIEW 2020, the 13th edition of the event, will be held at the Sands Expo and Convention Centre, Marina Bay Sands, Singapore, from 26 to 30 October 2020.

Singapore International Energy Week

Singapore International Energy Week (SIEW) brings together political, business, academic and energy industry thought leaders to advance solutions and actions across the energy spectrum of oil & gas, clean and renewable energy, and energy infrastructure financing. More information on SIEW can be obtained from www.siew.sg.

Energy Market Authority

Energy Market Authority (EMA) is a statutory board under the Ministry of Trade and Industry. EMA's main goals are to ensure a reliable and secure energy supply, promote effective competition in the energy market and develop a dynamic energy sector in Singapore. More information on EMA can be obtained from www.ema.gov.sg.

AIRCRAFT HANGAR OBTAINS

GREEN MARK PLATINUM (POSITIVE ENERGY) AWARD

An eco-friendly development by MINDEF, SAF and DSTA.

The hangar for the Republic of Singapore Air Force's (RSAF) A330 Multi-Role Tanker Transport (MRTT) aircraft is located at Changi Air Base (East).

In line with the whole-of-nation response to tackle climate change, the Ministry of Defence (MINDEF) and Singapore Armed Forces (SAF) are doing their part to be environmentally sustainable. Initiatives include the implementation of eco-friendly solutions such as the development of infrastructure with a focus on sustainable design, construction and operations, as well as utilising hybrid vehicles and food waste management.

Together with the Defence Science and Technology Agency (DSTA), MINDEF/SAF has incorporated green features upfront in the design of its new buildings. Besides making use of renewable energy and sustainable building materials, these facilities maximise water and energy conservation through water-efficient fittings as well as energy-efficient lighting and air-conditioning systems.

HANGAR FOR THE A330 MULTI-ROLE TANKER TRANSPORT AIRCRAFT

Completed in March 2020 at Changi Air Base (East), the hangar for the Republic of Singapore Air Force's (RSAF) A330 Multi-Role Tanker Transport (MRTT) aircraft is the SAF's first net positive energy building. For this achievement, the building obtained the Green Mark Platinum (Positive Energy) Award from the Building and Construction Authority (BCA) in February 2020.

The hangar will be able to generate 30% more electricity than it consumes. The additional electricity generated will be used to supplement other energy demands within the air base.

The development incorporates several green features:

Naturally ventilated interior space

The building is designed with a north-south orientation, to reduce heat gain. Airflow into the building is optimised for natural ventilation and a pleasant working environment, through vertically lifting, large front doors made of translucent, panelled fabric, and large-span louvres at the back of the hangar. High-volume low-speed fans further augment thermal comfort.

By allowing light to pass through, the translucent panelled fabric door also serves to reduce the artificial lighting requirements within the hangar.

Green roof

Besides serving as a rest and recreation area, a green roof also acts as an insulation layer to reduce solar heat gain into the building.

Sustainable building materials.

Eco-friendly products have been used in the construction of the building, such as low-VOC (volatile organic compounds) paint, green concrete, and other green materials each of which has been certified as a Singapore Green Building Product.

Power from renewable energy sources

The hangar uses solar PV panels as the source of renewable energy, to generate 1,225 MWh of electricity a year.

Energy-efficient design.

The building has an energy-efficient air-conditioning system and uses LED lighting, to conserve electricity.

Water conservation

Rainwater is harvested and recycled for general washing, auto-irrigation of the hangar's green roof, and flushing of toilets. Water-efficient fittings are also used, with total annual water savings estimated at 5,460 m³.

PROJECT CREDITS

Developer
Defence Science and Technology Agency

Architect
3HPArchitects Pte Ltd

Mechanical & Electrical Engineering Consultant
Bescon Consulting Engineers Pte

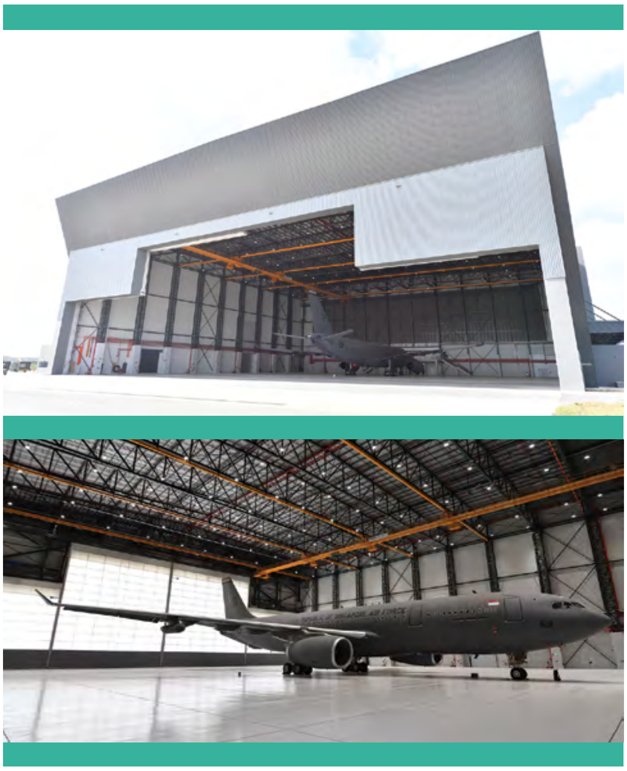
Environmental Sustainability Consultant
GreenA Consultants Pte. Ltd.

Civil & Structural Engineering Consultant
KTP Consultants Pte Ltd

Main Contractor
Sanchoon Builders Pte Ltd

All images by MINDEF

Rainwater is harvested and recycled for general washing, auto-irrigation of the hangar's green roof, and flushing of toilets, so as to conserve potable water.



The hangar with the panelled fabric doors lifted (image above) and lowered (image below). The translucent fabric doors allows natural light transmission into the building, thereby reducing the artificial lighting requirements.

Large-span louvres located at the back contribute to natural ventilation of the building.

The green roof acts as an insulation layer to reduce solar heat gain into the building.

SINGAPORE TEAMS RECOGNISED

FOR INNOVATIVE DESIGN AND ENGINEERING EXCELLENCE

The international competition for students to develop ultra-energy-efficient cars attracted more than 100 entries.

For Chng Tze Chen of Temasek Polytechnic (TP), cars have always been a fascination from a young age, while Peter Chong of Nanyang Technological University (NTU) is interested in creating practical solutions to improve current engineering mechanisms.

When the Shell Eco-marathon presented a chance to work on an actual car, they immediately jumped at the opportunity to represent their respective schools.

Although much of the world ground to a halt in early 2020, the spirit of student innovation and team work continued to shine brightly in the TP and NTU teams, eventually leading them to clinch the Technical Innovation Award and Vehicle Design Award (Urban Concept), respectively, at this year's Shell Eco-marathon Asia Off-Track Awards.

Shell Eco-marathon is one of the world's leading energy-efficiency competition programmes for science, technology, engineering and maths (STEM) students to design, build and drive ultra-energy-efficient cars.

Held virtually for the first time due to the pandemic, the Asian edition of the Off-track Awards continued its tradition of recognising excellence in communications, circular economy, technical innovation, vehicle design and safety.

This year's awards attracted more than 100 entries by 50 teams from 16 countries. The winners were announced in a virtual ceremony live on Shell Eco-marathon's Instagram and Twitter on 3 June 2020. Scuderia Ferrari Formula 1 Driver Charles Leclerc joined the ceremony as a special guest.

For the technical inventiveness of their vehicle design that recycles hydrogen waste to generate energy, TP Eco Flash impressed judges and bested competitors to receive the Technical Innovation Award for the first time.

While such systems exist in the market, hydrogen recycling is not widely adopted as the process consumes a considerable amount of power. Additionally, decompressors needed for such systems are often bulky and therefore not traditionally used in race cars or lightweight vehicles.

TP Eco Flash

TP Eco Flash gave themselves a challenge to address both areas. And the team succeeded, creating an innovation

TP Eco Flash testing their energy-conserving, purge-free hydrogen car at Temasek Polytechnic. Images: TP Eco Flash.

that requires less energy for recycling hydrogen while being compact enough to fit into an eco-car. Its purge-free capability also makes it safer than conventional hydrogen fuel cells.

A highly flammable gas, hydrogen could cause an explosion if accumulated in an enclosed space. To ensure safety, TP Eco Flash incorporated a fail-safe mechanism that would shut down the vehicle if hydrogen builds up as a result of not being recycled.

"Taking part in Shell Eco-marathon has been a very fulfilling journey for our team and our advisors, and we are glad that we were able to see our hydrogen-powered vehicle in action before the Circuit Breaker in Singapore happened. Being able to be part of this year's regional competition allowed us to test our ideas and come up with real-world solutions using clean energy. Our ability to effectively integrate knowledge from multiple disciplines - clean energy, electronics and mechatronics - to secure our win is certainly another plus", said Tze Chen, who is the student manager of TP Eco-Flash.

NV11 Nanyang Autonomous Venture

Another category that saw stiff competition was the Vehicle Design Award (Urban Concept). NV11 Nanyang Autonomous Venture from NTU made the strongest impression on panellists with the intricate details, overall packaging, quality interior and good ergonomics of their vehicle.

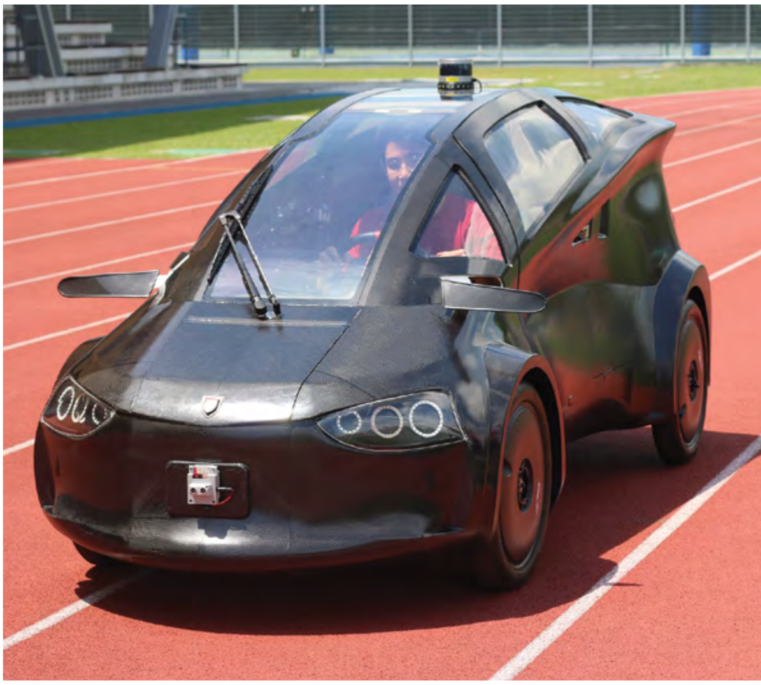
Inspired by the characteristic fusiform shape of the killer whale, or orca, which contributes to it being one of the fastest-swimming marine mammals, the electric eco-car boasts a streamlined, aerodynamic design, which reduces the drag from air moving past.

Modifying a design inherited from the NTU team that participated in Shell Eco-marathon 2019, the team of final-year undergraduates enhanced the steering, drivetrain, electrical and braking systems. The combination of these improvements increased energy efficiency by 30% to 40%, based on lab tests.

"I remember the day when we first took over the car from our seniors and each of us did a test drive to understand the areas for improvement. That experience got us really excited - a feeling that kept us going till the end, even when the COVID-19 pandemic meant that we could no longer compete on-track. Nonetheless, Shell Eco-marathon has provided a wonderful hands-on learning platform that allowed us to develop practical solutions to a present-day issue. We look forward to passing our knowledge on to subsequent NTU teams so that they can surpass and better our design", said Peter Chong, Lead Driver, of NV11 Nanyang Autonomous Venture.

This year also marks the 35th anniversary of Shell Eco-marathon. Over the years, Shell Eco-marathon has seen thousands of high school and university students from across the world build ultra-energy-efficient vehicles, in a variety of designs, using a spectrum of energy types. Every year brings new stories of human endeavour and technical excellence, as teams push the boundaries of what is possible.

In these extraordinary times, Shell Eco-marathon continued to find ways to keep the spirit of innovation alive among its student participants.



NV11 Nanyang Autonomous Venture and their killer whale-shaped eco-car. Images: NV11 Nanyang Autonomous Venture.

INDUSTRIAL-SCALE POWER-TO-HYDROGEN-TO-POWER DEMONSTRATOR LAUNCHED

The European technology driving the project is aimed at reducing carbon emissions.

With the HYFLEXPOWER project, a consortium made up of ENGIE Solutions, Siemens Gas and Power, Centrax, ARTTIC, German Aerospace Center (DLR) and four European universities are implementing a project funded by the European Commission, under the Horizon 2020 Framework Program for Research and Innovation. The implementation of this project, the world's very first industrial-scale power-to-X-to-power demonstrator with an advanced hydrogen turbine, will be launched at Smurfit Kappa PRF's site in Saillat-sur-Vienne, France. Smurfit Kappa PRF is a company specialising in the manufacture of recycled paper.

According to the ADEME (France's agency for environment and energy management), 'Power to X', or 'P2X', is the act of converting electricity into another energy vector. For the HYFLEXPOWER project, the 'X' vector is hydrogen.

The purpose of this project is to prove that hydrogen can be produced using electricity generated from renewable resources and it can be stored and then added to the natural gas currently used in combined heat and power plants, with the aim of ultimately achieving 100% replacement of the natural gas by hydrogen. For this, an existing Siemens SGT-400 industrial gas turbine will be upgraded to convert stored hydrogen into electricity and thermal energy, which can then be used to power a high-power industrial turbine.

Storing fluctuating renewable energy is one of the major challenges of the energy transition. In this context, the stakeholders involved in the HYFLEXPOWER project are developing new technologies which can be used across the whole power-to-X-to-power cycle. The installed demonstrator will be used to store excess renewable electricity in the form of green hydrogen. During periods of high demand, this stored green hydrogen will be used to generate electrical energy to be fed into the grid.

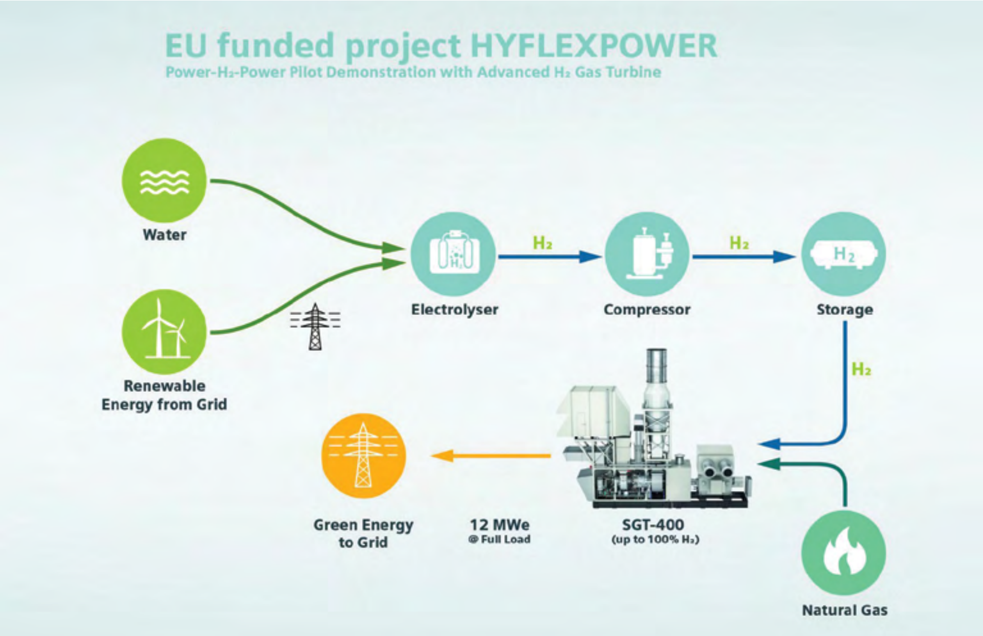
ENGIE Solutions has been entrusted with producing energy at the Smurfit Kappa site in Saillat-sur-Vienne, France. At the site, ENGIE Solutions operates a 12 MWe combined heat and power facility which produces steam for the manufacturing company's requirements. The conversion of an existing infrastructure has the advantage of significantly lower costs and minimised lead time compared to a greenfield site. The project will develop and demonstrate an advanced plant concept that will contribute to modernising and improving the factory's existing power plant.

During two demonstration campaigns, the facility will be powered by a mix of natural gas and hydrogen, ultimate-

A world first

Through its Horizon 2020 framework program, the European Commission supports highly innovative research and demonstration projects aimed at developing and creating innovative products and services and thus stimulating growth in Europe. For this, the European Commission is awarding grants based on a competitive procedure.

HYFLEXPOWER was able to assert itself against a large number of competitors for the grant. With this particular project, HYFLEXPOWER will demonstrate that renewable hydrogen can serve as a flexible means of storing energy


EU funded project HYFLEXPOWER
Power-H_2-Power Pilot Demonstration with Advanced H_2 Gas Turbine
Water
Renewable Energy from Grid
Electrolyser
H_2
Compressor
H_2
Storage
H_2
Green Energy to Grid
12 MWe @ Full Load
SGT-400 (up to 100% H_2)
Natural Gas

The purpose of HYFLEXPOWER is to prove that hydrogen can be produced and stored from renewable electricity and then added to the natural gas currently used with combined heat and power plants, with the aim of achieving 100% replacement of the natural gas by hydrogen.

ly aiming to achieve 100% hydrogen operation. In this regard, the overall goal of the HYFLEXPOWER project is to test an entirely green hydrogen-based power supply for a completely carbon-free energy mix. This would save up to 65,000 tons of CO_2 per year for a SGT-400 at baseload operation.

An exclusively European technology

The consortium selected, following the call for proposals, is made up exclusively of European companies and bodies. Each stakeholder's role is defined as follows:

- ENGIE Solutions will build the hydrogen production and storage facility, including the natural gas/hydrogen mixing station prior to the turbine.
- Siemens Gas and Power will supply the electrolyser for hydrogen production and develop the hydrogen gas turbine.
- Centrax will upgrade the package for hydrogen operation and install the new turbine.
- German Aerospace Center (DLR) together with the University College London, University of Duisburg-Essen and Lund University will support the hydrogen turbine technology development.
- National Technical University of Athens will perform economic, environmental and social assessments of the concept.
- ARTTIC will support the operational project management and the project’s communication activities.

The project's total budget is close to EUR 15.2 million, of which EUR 10.5 million will be contributed entirely by the European Union under the Horizon 2020 program.

Officially launched on 1 May 2020, the project will last 4 years and will be split into several phases:

- May 2020: Contract finalisation and start of engineering development.
- 2021: Installation of the hydrogen production, storage and supply facility at pilot demonstration site.
- 2022: Installation of the gas turbine for natural gas/hydrogen mixtures and initial demonstration of advanced pilot plant concept.
- 2023: Pilot demonstration with up to 100% hydrogen for carbon-free energy production from stored excess renewable energy.

This promising technology is fully in line with Siemens, ENGIE Solutions and Centrax’ strategy of providing its clients with zero-carbon solutions.

Helping to achieve decarbonisation

Siemens Gas and Power is helping its customers achieve their decarbonisation goals by building infrastructure for power-to-X-to-power and making a global contribution to cross-sector decarbonisation. Siemens offers all core technologies for a long-term CO_2-free energy supply, from power and heat generation, to power transmission and distribution, and efficient electrolysis for hydrogen production.

“Siemens Gas and Power wants to be the driving force behind the decarbonisation of energy systems worldwide. Our goal is to make our gas turbines usable for 100% hydrogen. With that, our gas turbines can be the ‘technology of choice’ for our customers to complement the intermittence of renewables and ensure a secure energy supply in the decarbonised world of the future”, said Karim Amin, CEO of the Generation Division of Siemens Gas and Power.

A stakeholder committed to hydrogen

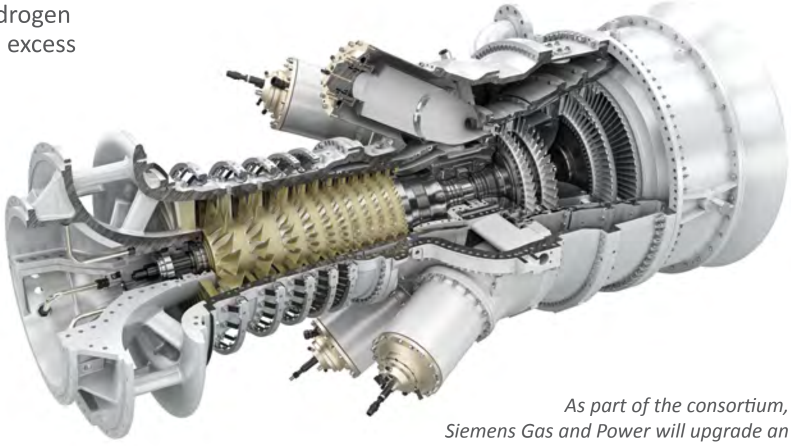
As an energy for the future, green hydrogen has a major role to play in the energy transition. For ENGIE Solutions, the most abundant element in the universe is vital to decarbonising industrial processes. ENGIE Solutions is certain that this energy will help speed up the transition of regions and manufacturing companies and is supporting the development of renewable hydrogen. The company already has a number of projects, either in operation or forthcoming.

"With the HYFLEXPOWER project, ENGIE Solutions is once again demonstrating its intent to support manufacturers and regions as they seek to optimise and green their energy use. Developing renewable hydrogen for industrial purposes is a perfect example. This demonstrator is the future”, said Pierre Hardouin, CEO of ENGIE Solutions for Industries.

Developing hydrogen-ready solutions

Centrax sees ‘green hydrogen’ as an important part of the path to a decarbonised energy system and welcomes the considerable investment being made by the Horizon 2020 program to assist the development of hydrogen compatible combustion systems.

“Our goal is for our gas turbine combined heat and power systems to be ‘hydrogen ready’ to provide future-proof power generation solutions for our customers”, said Harry Trump, Director of Business Development for Centrax Ltd.



As part of the consortium, Siemens Gas and Power will upgrade an existing SGT-400 industrial gas turbine to generate electricity and thermal energy with stored hydrogen and demonstrate an industrial-scale power-to-hydrogen-to-power solution.

MAXIMISING THE TOTAL EFFICIENCY OF OFFICES

A leading international HVAC company explains how this can be achieved.

Throughout history, humankind used to work primarily outdoors. The new reality is that we spend most of our working lives indoors. The statistics from the National Human Activity Pattern Survey (NHAPS) show that people spend approximately 90% of their waking hours indoors [1]. Furthermore, average people spend over 13 years of their lives at work according to one analysis from HuffPost Australia [2].

At the same time, advances in technology have reshaped our daily lives. Cities are becoming smart, buildings are becoming smart, and the future workplace is becoming smart. According to 'Top 6 Future Work Trends' by Gartner, a global research and advisory firm, physical workplaces can become smart.

The evolution of HVAC systems, which is one of the key elements of the building management system, is in line with this trend. There are three necessary conditions to be fulfilled for HVAC systems to become smart. They should:

- Increase the productivity of employees.
- Meet the needs of office buildings.
- Promote both energy efficiency and economic efficiency.

Healthy air to boost business performance

On average, people spend eight hours a day in the office. Therefore, it is obvious that Indoor Air Quality (IAQ) of the office will affect business performance.

In 2015, a study conducted by Harvard T H Chan School of Public Health and United Technologies Climate, Controls & Security found that productivity and IAQ in the office are strongly linked [3].

Comparing the performance of employees working in 'healthy air' to those working in 'polluted air', the former group made an additional USD 15,500 per year.

Furthermore, cognitive functions improved by 50% when the CO_2 level in the office was lowered from the normal concentration of 1,400 ppm to 600 ppm, according to a study by Harvard T H Chan School of Public Health [4].

Therefore, offices need to manage the IAQ and keep the set temperature, by adjusting the wind direction automatically or utilising a sensor to detect when no one is present and stop operation of the air-conditoner.

Customised zoning to satisfy the needs of buildings

From large office buildings to government offices and apartment-type factories in a city, modern workplaces vary in kind. Even a single work environment is composed of several distinct spaces that meet the needs of various kinds of work. Therefore, flexible offices require HVAC systems optimised for the orientation of the building and the interior space characteristics.

For example, IberEspacio, based in Spain, designs and manufactures thermal control hardware for spaces. The company's biggest challenge was interior climate control for offices and laboratories. As a result, IberEspacio chose the HVAC system that could flexibly manage the airflow depending on the use of the space.

In the case of office buildings located in the middle of a city, there are many environmental challenges to overcome due to the surrounding buildings and the floating population. WeWork, a global commercial real estate company providing shared workspaces, proceeded on a renovation project at the Aviation House office space in London. Taking regional characteristics into consideration, the office installed an HVAC system that met the allowable noise level without losing capacity [5].

Maximising energy- and cost-efficiency

According to the European Commission's 'Energy performance of buildings directive', buildings are responsible for 40% of energy consumption in Europe [6].

The US Energy Information Administration (EIA) also says commercial buildings consume a large portion of energy in the US, due to the increased use of existing electrical equipment and the introduction of new types of office equipment and telecommunication equipment.

Fortunately, advancements in HVAC systems can help building owners save energy, by predicting future energy consumption, with the help of solutions such as LG Electronics' LATS energy program, and building energy modelling products including eQuest, EnergyPro and Trace700.

CIBIS Tower 9, a landmark and LEED Platinum certified building in Jakarta, Indonesia, required a highly efficient air-conditioning system that could reduce the operational energy consumption. The building chose the best solution by simulating and comparing the energy consumptions, before installation.

CIBIS Tower 9 could also save costs, with the efficiencies achieved in the design, development and construction stages. As the building introduced a total HVAC solution, the client could benefit from a smooth maintenance service. Furthermore, an accurate billing system for each tenant also helps to prevent unnecessary costs.

Customised HVAC system for the office

LG Electronics has released a line of customised HVAC systems to improve the efficiency and bring down the TCO (Total Cost of Ownership) of the office.

The company has introduced the Multi V series to provide the benefits of Variable Refrigerant Flow (VRF) to office buildings.

To improve the working environment, LG offers Multi V AHU and Multi V Dual Vane 4 Way Cassette. Multi V AHU, providing ventilation with cooling and heating, maintains a constant CO_2 concentration to provide pleasant indoor air.

Multi V Dual Vane 4 Way Cassette adjusts the temperature of both direct and indirect wind, to create a comfortable and efficient working environment. Plus, the cassette provides clean air with the company's advanced air purifying kit and panel, achieving a Clean Air Delivery Rate (CADR) of 692.2 ft^3/min [7].

LG's HVAC system benefits consultants with products that take into account space characteristics. With one outdoor unit, Multi V 5 can provide both cooling and heating at the same time. For example, Multi V 5 can provide cooling in a computer room and a communication device room with a high heat output, while simultaneously provide heating in general office rooms. This would be of value to countries with seasonal cold weather. In this way, the flexible, functional and multipurpose needs of the building can be satisfied.

Also, LG provides technical support and service throughout the installation process and after, including onsite training for the customer's installation team. This is of great help to both building owners and consultants. In adition, LG offers 'Energy Simulation Analysis' to help customers compare energy consumption patterns.

"As the industry evolves, offices and HVAC systems are also undergoing a transformation", said Junhyuk Seong (Justin), Head of the Product Management / Air Solutions, LG Electronics Singapore.

"LG Multi V is an efficient VRF with great flexibility. It is the best solution for offices [to ensure] user comfort and [encourage] maximum concentration of employees", he added.

REFERENCES

[1] Neil E Klepeis et al: 'The National Human Activity Pattern Survey (NHAPS): A Resource for Assessing Exposure to Environmental Pollutants', 15.

[2] 'We've Broken Down Your Entire Life Into Years Spent Doing Tasks', HuffPost Australia, last modified Oct 19, 2017, accessed Apr 28, 2020, https://www.huffingtonpost.com.au/2017/10/18/weve-broken-down-your-entire-life-into-years-spent-doing-tasks_a_23248153.

[3] Piers MacNaughton et al: 'Economic, Environmental and Health Implications of Enhanced Ventilation in Office Buildings', 14718.

[4] Joseph G Allen et al: 'Associations of Cognitive Function Scores with Carbon Dioxide, Ventilation, and Volatile Organic Compound Exposures in Office Workers: A Controlled Exposure Study of Green and Conventional Office Environments', 810.

[5] Based on results from LG's internal CFD analysis.

[6] Energy performance of buildings directive, European Commission, last modified Mar 12, 2020, accessed Apr 28, 2020, https://ec.europa.eu/energy/topics/energy-efficiency/energy-efficient-buildings/en-ergy-performance-buildings-directive_en.

[7] Certification by Korean Air Cleaning Association (KACA, http://www.kaca.or.kr)

Images by LG Electronics Singapore

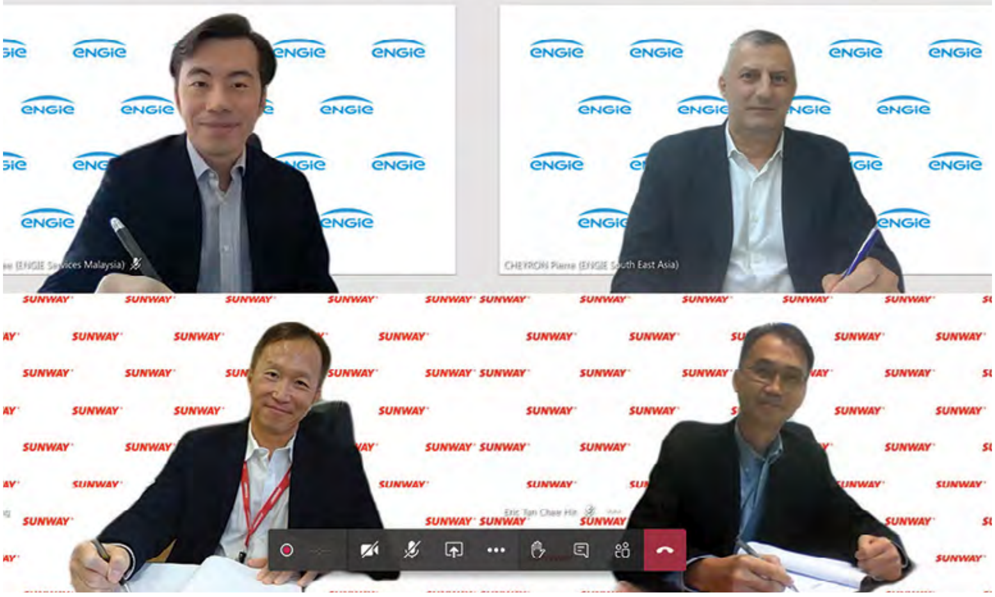
The Multi V 5, from LG, provides high energy efficiency while minimising operational costs. Its dual sensing control senses temperature and humidity.

The Multi V S, from LG, is a compact yet powerful VRF for private residences and small offices, that provides maximised energy efficiency with low operation costs.

EXPANDING DISTRICT COOLING TECHNOLOGY IN MALAYSIA

It is expected to help achieve environmental sustainability goals.

ENGIE South East Asia and Sunway Construction Sdn Bhd, Malaysia, a wholly-owned subsidiary of Sunway Construction Group Berhad (SunCon) recently announced that they have signed a Memorandum of Understanding (MoU) to set up a joint-venture company (JVCo) to boost Malaysia's environmental sustainability effort. SunCon is part of Sunway Group (Sunway), one of Malaysia's largest conglomerates with core interests in real estate, construction, education, healthcare, retail and hospitality.



The MoU between ENGIE South East Asia and Sunway Construction Sdn Bhd, Malaysia was signed by, in the top row, from left to right, Wong Yin Kee, Deputy Managing Director, ENGIE Services Malaysia and Pierre Cheyron, Chief Executive Officer, ENGIE South East Asia, and in the bottom row, from left to right, Liew Kok Wing, Managing Director, Sunway Construction and Eric Tan, Executive Director, Sunway Construction.

The JVCo will engineer, finance, construct, develop, operate and maintain district cooling systems for greenfield and brownfield urban development projects, including some of ENGIE South East Asia Pte Ltd.

Sunway's portfolio includes office buildings, retail malls, educational institutions, medical centres, hotels, resorts, theme parks and factories. The JVCo will also leverage Sunway's capabilities and experience as a conglomerate with 13 business divisions, and the core business and technical competencies of ENGIE in integrated green and sustainable environmental solutions.

The partnership will contribute towards accelerating the adoption of district cooling technology in Malaysia. This is in line with Sunway's commitment towards advancing the United Nations Sustainable Development Goals (UN-SDG), particularly Goal 7: Affordable and Clean Energy.

District cooling systems

Globally, district cooling systems are becoming the preferred cooling solutions for cities and buildings, as compared to stand-alone chiller plants. District cooling produces chilled water centrally for distribution to nearby facilities through a network of insulated pipes to achieve efficient air-conditioning of buildings.

This technological approach is said to be more efficient and generates significant savings in capital expenditures, energy and operating costs compared to the conventional usage of de-centralised chiller plants. District cooling is a key enabler in meeting the increasing air-conditioning needs of businesses and customers in a more sustainable way for the environment, in Malaysia and in ASEAN.

ENGIE's project portfolio includes 393 district heating and cooling networks globally, including, in Southeast Asia, the Megajana District Cooling System, Cyberjaya, Malaysia; Northgate District Cooling Plant, Philippines; and the District Cooling Systems for Punggol Digital District in Singapore.

Sunway Construction Group

Sunway Construction Group Berhad (SunCon) is Malaysia's largest pure-play construction group and is listed on Bursa Malaysia. As an award-winning group, SunCon has built on its expertise and experience for nearly four decades.

ENGIE South East Asia

ENGIE South East Asia, a cluster under ENGIE Asia-Pacific, has a presence in Singapore, Malaysia, Thailand and the Philippines, to provide tailor-made solutions for commercial buildings, industries and cities. The ENGIE Group is a leader in low-carbon energy and services.

TOWARDS ZERO RESUBMISSIONS

An initiative from PUB, Singapore's National Water Agency, will help to increase productivity in building projects.

Introduction

Very often, professionals employed by building owners, developers, architectural firms, engineering consultancies and contractors, need to make multiple resubmissions to PUB because their designs are not compliant with the PUB Code of Practice requirements.

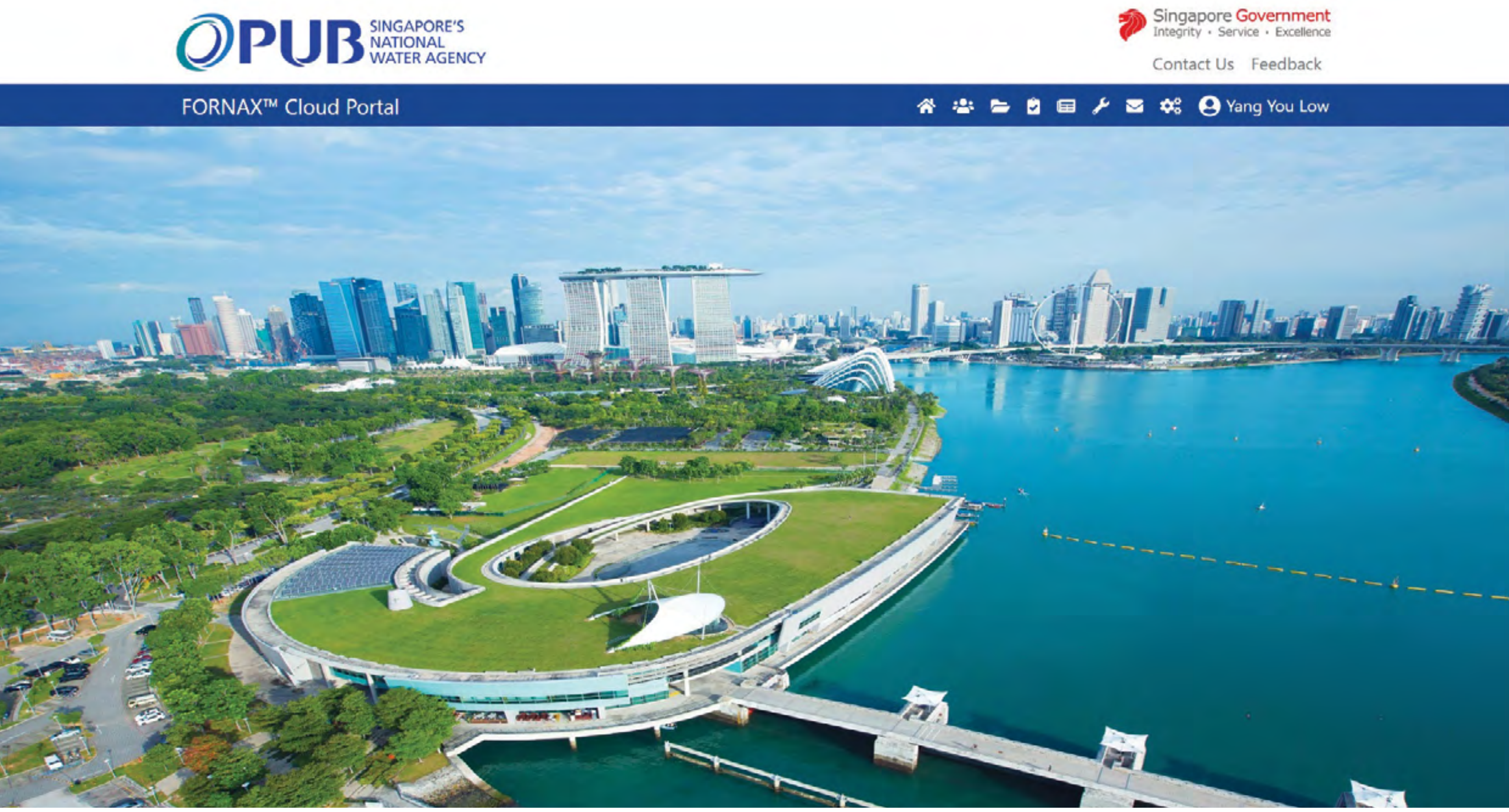
To avoid having to make such resubmissions, PUB has launched the Building Information Modelling e-Checker System (BIM e-Checker).

Developed in consultation with industry professionals, the BIM e-Checker automatically checks BIM submissions in open BIM format (IFC) for compliances with standing regulations, guidelines and Code of Practices, and is capable of generating the results of the checks quickly. Checks can be conducted at any time of the day, by simply uploading the open BIM formatted (IFC) designs into the system.

BIM e-Checker user comment

"The user-friendly BIM e-Checker software has helped us to quickly identify non-compliances and allowed us to make the necessary changes to our BIM models before we make formal submissions to PUB. The software allows us to identify and address all non-compliances, thereby reducing the time taken for approval.

The BIM e-Checker initiative from PUB to support the industry is a positive development as this would ensure that designs are compliant and designers can focus on value-adding for their clients, instead of worrying about non-compliance issues during design." - Clement Toh, JTC



The main page of PUB's BIM e-Checker Portal.

Phase 1 of the BIM e-Checker, which covers checks on all prescriptive PUB requirements, has been made available from 15 April 2020.

Subsequent CORENET processing of these plans will be accorded priority, since they are fully compliant with the e-Checks.

The PUB BIM e-checker

The PUB BIM e-checker is a system developed as a value-added tool, to help industry users self-check their BIM models (IFC) for compliance against PUB Code of Practice requirements, before formal submission via CORENET.

The user is required to create an account at the portal (https://Buildingplanchecker.pub.gov.sg). How-to guides are available on the portal for the user's reference.

Benefits to users

The system aims to generate results within 24 hours after the model has been uploaded. However, the rule for checking needs to be selected accordingly.

Since the PUB BIM e-Checker will allow users to make sure their designs are compliant with PUB Code of Practice requirements, before formal submission to PUB via CORENET, it will mean less resubmission and, consequently, productivity will be improved in the project.

Making a CORENET submission

The current modelling guide is published for Revit and ARCHICAD. To use the BIM e-Checker, the models need to be converted into IFC 2x3 format, in order to support interoperability. For other BIM authoring software, guides will be published progressively.

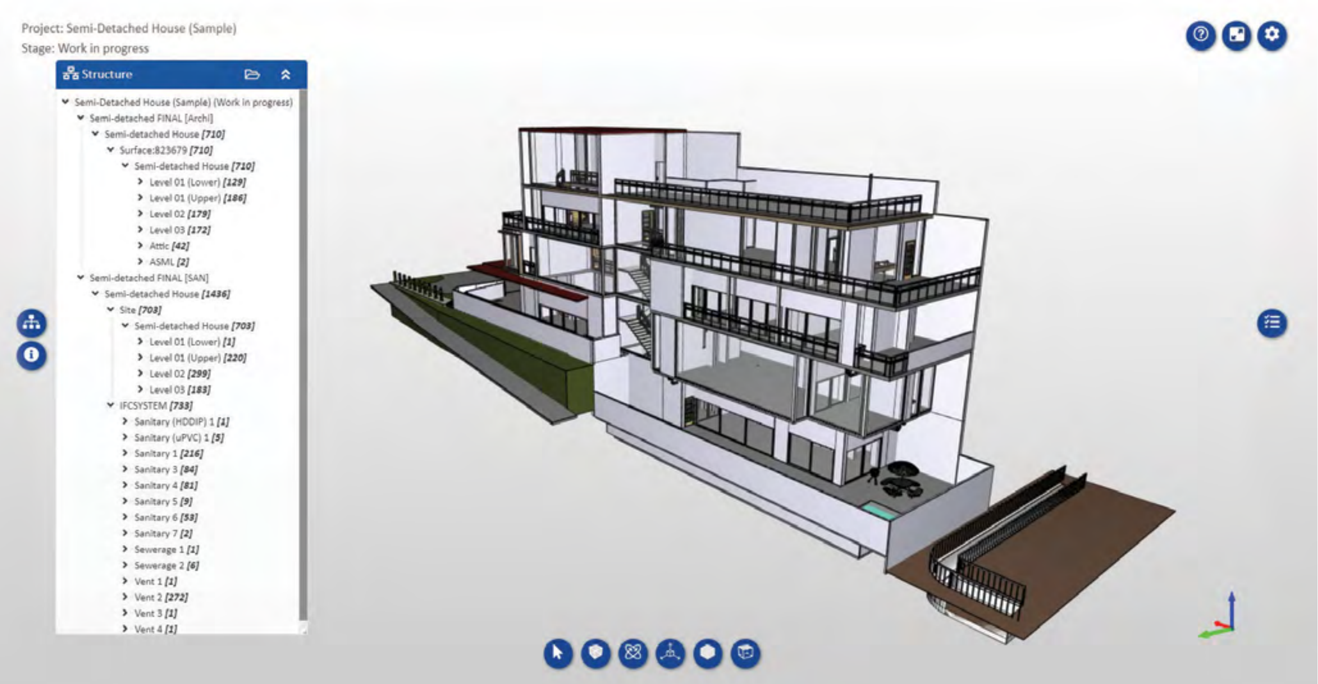
BIM e-Checker user comment

"By using the BIM E-checker software, the non-compliances can be revealed quickly. The reports generated in BCF format give a quick identification of the location of the non-compliances and we can link the BCF back to the native model for easy identification of the non-compliant items and make amendments in the model for a formal submission.

There is also some reduction in the time taken for the approval process as the obvious non compliances are identified early, so that re-work can be done earlier. However, in the trial session for the online submission process, we noticed that the time taken for a response to the online submission depends on the model sizes, the code of compliances/rules lists that are selected for the online review. So the actual online review time varies in length.

The BIM e-checker is quite easy to use, provided that the user has mapped the IFC schema/space information to the PUB standard. In view of this, there will be a need for the user to spend time to update the in-house project template and adopt the PUB object parameters.

In general, the PUB template and the guides provided are useful. However, we have noticed that some PUB object file sizes are too large, and the naming of objects is not based on ARCHICAD default naming. The object library could be provided as an external LCF file for linking (to reduce file size) etc."
- Chung Yok May, P & T Consultants Pte Ltd



Project: Semi-Detached House (Sample)
Stage: Work in progress

3D building models in IFC format can be viewed on the BIM e-Checker portal.

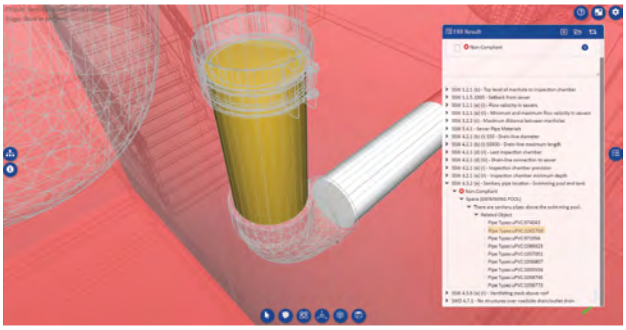
After performing a check using the PUB BIM e-checker, the user can make a CORENET submission as per normal. The compliant report from the BIM e-Checker and the relevant IFC files are to be included in the submission. The submission number must also be emailed to pub_bpu@pub.gov.sg. If the IFC file is too large for submission through CORENET, a link should be provided for PUB to download the IFC. Only submissions supported by the checking report will be processed.

If there is a non-compliance due to site constraints, PUB should be consulted.

Briefing and training

Briefing and training will be provided for users to familiarise themselves with the usage of the portal - from creation of the model, to uploading it and to reviewing of results. More details will be shared at a later date.

In the meantime, users can refer to the modelling guide and how-to videos available on the BIM e-Checker portal.



FXR Result

□ Non-Compliant

- SSW 1.2.1 (b) - Top level of manhole to inspection chamber
- SSW 1.2.5.1000 - Setback from sewer
- SSW 3.2.1 (e) (i) - Flow velocity in sewers
- SSW 3.2.1 (e) (ii) - Minimum and maximum flow velocity in sewers
- SSW 3.2.2 (c) - Maximum distance between manholes
- SSW 3.4.1 - Sewer Pipe Materials
- SSW 4.2.1 (b) (i) 150 - Drain-line diameter
- SSW 4.2.1 (b) (i) 50000 - Drain-line maximum length
- SSW 4.2.1 (d) (ii) - Last inspection chamber
- SSW 4.2.1 (d) (iii) - Drain-line connection to sewer
- SSW 4.2.1 (e) (i) - Inspection chamber provision
- SSW 4.2.1 (e) (ii) - Inspection chamber minimum depth
- SSW 4.3.2 (a) - Sanitary pipe location - Swimming pool and tank
  - Non-Compliant
    - Space (SWIMMING POOL)
      - There are sanitary pipes above the swimming pool.
        - Related Object
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
          - Pipe Types:uPVC:[illegible]
- SSW 4.3.6 (a) (ii) - Ventilating stack above roof
- SWD 4.7.1 - No structures over roadside drain/outlet drain

Non-compliant result: Sanitary pipes should not be located above swimming pools.

The use of the PUB BIM e-Checker is not mandatory, as yet.

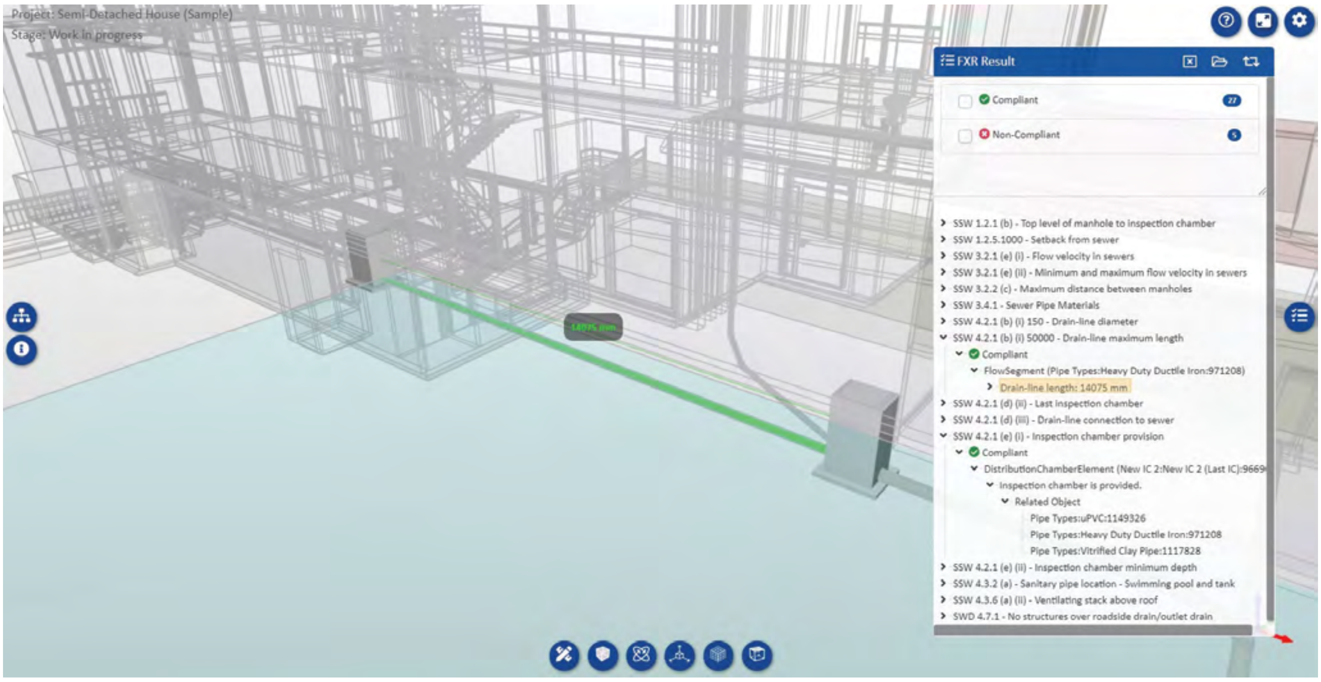
(More information may be obtained from https://Buildingplanchecker.pub.gov.sg)

BIM e-Checker user comment

"Traditionally, code compliance checking is carried out by manual observations. Modern building design is getting more complex with the advancement of 3D modelling technology and fast-paced project delivery. This is posting a challenge to manual checking. The development of an automation application like the BIM e-Checker is helpful and is being welcomed by the industry. It can help designers to quickly identify non-compliances, especially during the design iteration process, before finalising the formal submission.

The current version of BIM E-checker is easy to use. It can be made better with improvements in the visual design aspects and in the interaction with users. Animation showing step-by-step guides, as well as hover effects providing tips or descriptions of clickable tools, can create a soothing environment. An embedded chatroom would be convenient for users who need to ask questions."
- Lim Kok Keong, ONG&ONG Group

Images by PUB, Singapore's National Water Agency



Project: Semi-Detached House (Sample)
Stage: Work in progress

FXR Result

□ Compliant 27

□ Non-Compliant 5

- SSW 1.2.1 (b) - Top level of manhole to inspection chamber
- SSW 1.2.5.1000 - Setback from sewer
- SSW 3.2.1 (e) (i) - Flow velocity in sewers
- SSW 3.2.1 (e) (ii) - Minimum and maximum flow velocity in sewers
- SSW 3.2.2 (c) - Maximum distance between manholes
- SSW 3.4.1 - Sewer Pipe Materials
- SSW 4.2.1 (b) (i) 150 - Drain-line diameter
- SSW 4.2.1 (b) (i) 50000 - Drain-line maximum length
  - Compliant
    - FlowSegment (Pipe Types:Heavy Duty Ductile Iron:971208)
      - Drain-line length: 14075 mm
- SSW 4.2.1 (d) (ii) - Last inspection chamber
- SSW 4.2.1 (d) (iii) - Drain-line connection to sewer
- SSW 4.2.1 (e) (i) - Inspection chamber provision
  - Compliant
    - DistributionChamberElement (New IC 2:New IC 2 (Last IC):9669
      - Inspection chamber is provided.
        - Related Object
          - Pipe Types:uPVC:1149326
          - Pipe Types:Heavy Duty Ductile Iron:971208
          - Pipe Types:Vitrified Clay Pipe:1117828
- SSW 4.2.1 (e) (ii) - Inspection chamber minimum depth
- SSW 4.3.2 (a) - Sanitary pipe location - Swimming pool and tank
- SSW 4.3.6 (a) (ii) - Ventilating stack above roof
- SWD 4.7.1 - No structures over roadside drain/outlet drain

Compliant result: Sanitary drain-line meets the maximum 50 m length requirement.

HELPING TO MEET THE DEMANDS OF SOCIAL DISTANCING

A global leader is providing full access to relevant software to mitigate risk in re-opening public facilities

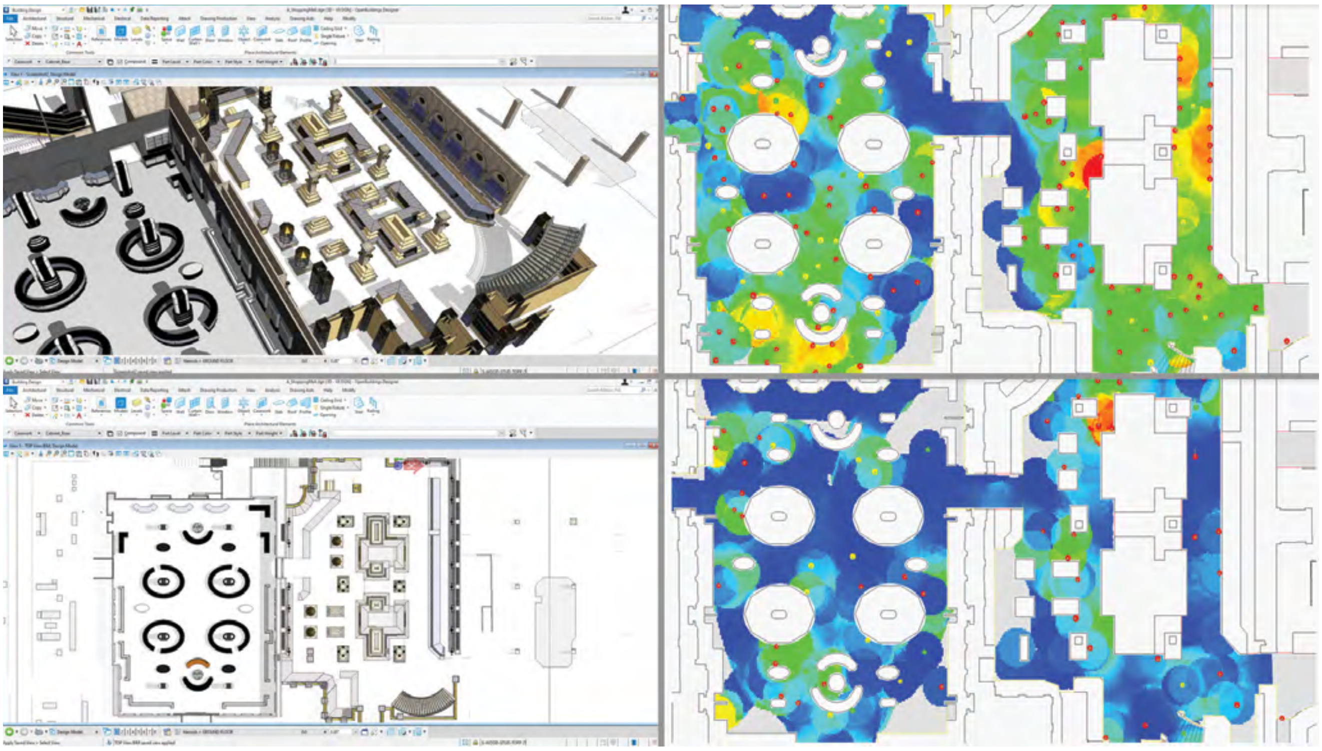
Bentley Systems Incorporated, a leading global provider of comprehensive software and digital twins services for advancing the design, construction, and operations of infrastructure, recently announced it has opened up its LEGION Simulator and OpenBuildings Station Designer software, including waiving new subscription fees through 30 September 2020, for facilities managers to incorporate pedestrian simulation methodologies across their planning, design, and operations teams.

With social distancing and crowd management at the forefront of global concerns, OpenBuildings Station Designer and LEGION Simulator software can help station owners, planning and design firms, and facilities operators to develop models, simulate crowd movement, analyse foot traffic, and optimise space utilisation of infrastructure assets such as rail and metro stations, airports, retail and commercial complexes, hospitals, and stadiums. OpenBuildings Station Designer's BIM environment provides 3D context for LEGION's included pedestrian simulation to create an operational digital twin to improve safety, efficiency, and security, while mitigating risk.

LEGION Simulator helps users solve new planning and operations challenges relating to the following:

- Validating social distancing plans while helping to ensure safe operations.
- Ensuring space maximisation, activities distribution and controlled egress/ingress.
- Modelling safe and comfortable wayfinding strategies and evacuation plans.
- Providing virtual, collaborative planning, design and operations reviews.

Further, LEGION Simulator and OpenBuildings Station Designer offer the continued long-term benefits of a BIM collaboration environment that avoids data silos, coordination delays, and other limitations that result from the separation of planning and design workflows.



The image on top left illustrates a 3D model of a retail operation created using OpenBuildings Station Designer. The image on bottom left shows 2D floor plans that are then imported into LEGION Simulator (the two images on the right) to test two scenarios. Examples shown are at occupancy rates of 75% (image on top right) and 25% (image on bottom right) to comply with social distancing requirements.

"We are going through extraordinary times and change will be a constant reality in the months and years ahead. Bentley's OpenBuildings Station Designer and LEGION Simulator enable planners, architects, engineers, and operators to apply digital twin approaches to solve today's design and operation challenges more quickly, efficiently, and safely across rail and metro stations, airports, and other public buildings and amenities", said Ken Adamson, Vice President, Design Integration for Bentley.

"Atkins has collaborated successfully with LEGION for over 20 years, and we look forward to building upon our own thought leadership on Covid-19 and for the Transport Sector by applying LEGION's simulations for social distancing in response to requests by our metro clients in Hong Kong, Singapore, Dubai, and Saudi Arabia", said Cameron MacDonald, Technical Director, Operations Advisory, Atkins, a member of the SNC-Lavalin Group.

LEGION and OpenBuildings Station Designer are part of Bentley's comprehensive efforts to provide resources and useful information to help both user organisations and end-users meet the current challenges successfully.

OpenBuildings Station Designer

OpenBuildings Station Designer enables professionals of multiple disciplines, including planners, architects and mechanical, electrical and structural engineers, to collaborate in real-time to design, analyse, visualise, and simulate infrastructure assets such as rail and metro stations, airports, retail and commercial complexes, hospitals, and stadiums. Projects of any size, form, and complexity can benefit and it is said to be the only design application to fully integrate people movement simulation, via LEGION Simulator.

LEGION Simulator

LEGION Simulator enables fast and scientifically validated evacuation simulation, for baseline operations and for any what-if scenario that operations teams may wish to test. It can seamlessly validate new entrances and exits, queuing strategies, flow separation barriers, and any other physical or operational changes in public spaces. Users can reduce risk and enhance the safety of their facilities through single source of truth models that enable easier collaboration and alignment between planning, design, operations, and safety teams.

OpenBuildings Station Designer helps designers improve the quality of station and facility design and optimise the functional use of space and the pedestrian experience.

COVID-19 PANDEMIC HIGHLIGHTS THE NEED FOR SMARTER AND MORE ADAPTABLE CITIES

by Cedrik Neike, CEO, Siemens Smart Infrastructure

Solutions must be found that are human-centric and resilient in the face of unforeseeable challenges.

Mr Cedrik Neike

The coronavirus pandemic is a new experience for every one of us. It has changed life as we know it - at work, at home and in public interactions. As some countries start to ease restrictions on public life, how can we go back to the 'normal' while still maintaining social distancing and feeling safe? How do we manage crowded public spaces like shopping malls, cinemas and restaurants? How do we optimise safety in our offices and factories? More importantly, how do we avoid shutting down entire cities and countries when the next pandemic hits?

Adaptability as the game changer

Many would argue there are very few, if any, human-centric cities in the world. The reasons for this include air pollution, poor urban planning and traffic congestion, to name a few. However, despite the chaos of the past months, I am convinced there is a silver lining - it is in adaptability. It is now clearer than ever that the main characteristic of our future cities needs to be adaptability.

Here is why I believe this is so:

The pandemic has given our environment a much-needed breather, but it has not removed the biggest challenges we are up against. Our resources are still finite, and using them efficiently so we can live sustainably on this planet remains a top priority.

Today, we have a golden opportunity to reassess how technology can be applied to tackle the challenges of climate change, urbanisation and population growth. The pandemic is creating a paradigm shift. We are on the cusp of a leap into a new era of digitalisation.

While 99% of city infrastructure remains dumb today, technologically speaking, digitalisation can make it more flexible and quicker in responding to crises. Digitalisation allows us to create a digital, adaptable twin of a city in the virtual world. We can test and simulate a city's resiliency to events like natural disasters and pandemics. This helps us understand how adaptable it is to such events and simulate a number of responses to activate in the future.

Our goal should be to create cities that balance environmental impact and economic growth. While natural resources continue to dwindle, data is an infinite resource at our disposal. Data is at the heart of digitalisation. Using it can help us achieve this goal by eliminating waste and saving energy and cost. We are already doing that in buildings - and getting better at it. But leveraging data to the advantage of people in cities is still at its infancy. In the future, we envision smart infrastructure becoming all-sensing and an ecosystem that knows you and adapts to your needs, thanks to data and digitalisation.

This process is continuous - in the sense that we should create an infinity loop, that is, constant improvement based on the connection from the physical and virtual worlds. It is like children whose brains develop based on sensory experience - gaining knowledge through feedback from senses, for example, their learning not to touch something hot. The infinity loop for infrastructure connects input from all the sensors and experts to continuously improve the experience of those in the city and enhance the value of solutions for our customers.

All-sensing infrastructure

Sensors make all-sensing infrastructure possible. They are used almost everywhere today, from detecting earthquakes, to measuring your heart rate on a fitness tracker and to ensuring safety of workers on industrial sites. Data collected through these sensors is sent to a computer to be analysed and used intelligently.

The COVID-19 pandemic has emphasised, even more, the need for adaptable cities.

The significance of sensors is growing and is only going to increase after this pandemic, with intelligent sensors contributing more to our public and private lives. This is because they allow us to monitor our surroundings like never before. The challenge is to create an ecosystem by joining all the dots.

Today, through our subsidiary, Enlighted, smart sensors collect and monitor real-time occupancy, light levels, temperatures and energy use. Enlighted is a leading provider of Internet of Things (IoT) solutions for commercial buildings.

The smart sensors can distinguish between people and objects and customise controls for specific purposes. There are 3.5 million sensors installed across our customers' buildings, globally, helping them make the best use of their office space and cut energy costs. In the UK, they enable an NHS outpatient facility to cut energy spend by 80% annually.

Smart sensors are also useful in case of a fire - giving firefighters reliable information about the number of people and their location in the building. In other cases, they monitor air pollution, helping cities comply with clean air and emission reduction targets.

While in the past, we placed sensors to protect and operate our infrastructure, now we are extending that to make our environment anticipatory, interactive and caring. We realise that using smart IoT sensors can significantly contribute to secure business continuity during a pandemic.

Possible future applications of sensors

What if a pandemic hits again? Sensors could help us continue to work in the office and meet in public by enabling social distancing. They can quantify the density in any given area at any given time, making sure people keep their distance and avoid overcrowding. This means we may not have to shut entire cities and countries in the future.

We also expect the focus on office space efficiency and utilisation to increase. It is something we have looked at for different use cases, such as comfort or asset efficiency, for a while. In response to COVID-19, more customers are asking for applications that help them design their offices in more optimal ways.

Today, 33% of commercial real estate space is underutilised or unused, creating an opportunity to save cost. Add to this the opportunity for a significant increase in ongoing home working, thanks to the biggest 'forced test' in history, and the potential for reducing real estate costs becomes compelling.

There could also be more demand for critical environment applications, for example, in pressurised rooms for hospitals and labs. In indoor spaces, often more polluted than outdoors, we can use occupancy data to adjust airflow, so it circulates better when there is a high density of people in one area. This ensures better air circulation in supermarkets, for example.

Imagine coming to the office during a pandemic. How do we ensure infected people stay at home? Sensors can also play an important role here by measuring temperature and communicating with access control systems. Workplace apps, such as Comfy, can play a role, allowing people to book only desks that are 2 m apart from the next occupied desk.

Ethical smart infrastructure

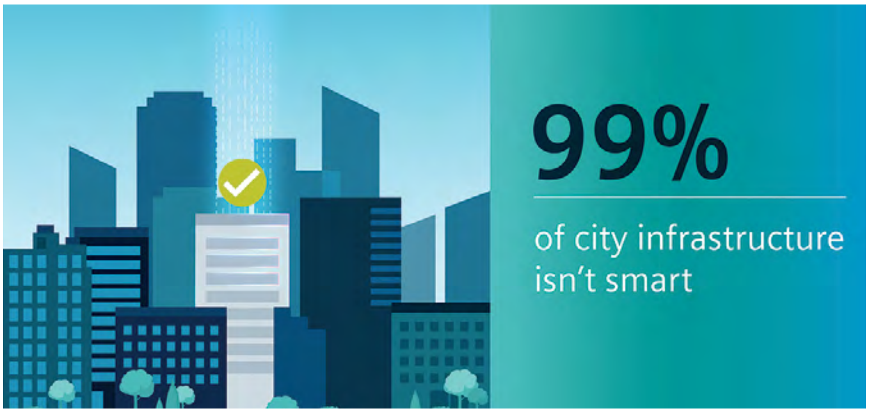
But more sensors in smart cities also raises important ethical concerns around data privacy - even if our sensors ensure anonymity.

Data privacy is about balancing what is feasible, legal and ethically right. If we want to create all-sensing infrastructure that helps preserve natural resources and tackle global challenges, we need to collect and analyse data. There will be hard choices to make - privacy versus safety, environmental impact and convenience. Individuals have the right to decide what matters to them. We want to make sure our data is used for the limited purpose we signed up to and not misused. Global companies have a big responsibility to manage data ethically and show transparency about what is stored and for what purpose.

Benefitting from what we have learned

In summary, our world has changed forever. Let us create a new normal that benefits from new uses of technology and from the positives of the experiences of lockdown. We must take the time to reflect on what we want to take forward - more home working, increased virtual collaboration, fewer air miles and corresponding carbon footprint reduction, flexible working to gain more hours with family, and even a recognition of what really matters in life.

Data exchange will be key to making our cities more adaptable and resilient to crises, whether they are caused by pandemics or natural disasters or by climatic change. With the right setup, the infrastructure that is most adaptable to change will not only survive but also help society to thrive.



Digitalisation can make city infrastructure more flexible and quicker in responding to crises.

PANDEMIC RESPONSE TECHNOLOGY

INITIATIVE TO COMBAT CORONAVIRUS

An international leader in semiconductor technology is accelerating access to technology to combat the current crisis and enable new scientific discoveries that could help in future situations.

Intel has pledged an additional USD 50 million in a pandemic response technology initiative to combat the coronavirus through accelerating access to technology at the point of patient care, speeding scientific research and ensuring access to online learning for students. Included in Intel's effort is an additional innovation fund for requests where access to Intel expertise and resources can have immediate impact. This is in addition to prior announcements of USD 10 million in donations that are supporting local communities during this critical time.

Allocation of the funds

Approximately USD 40 million will fund the Intel COVID-19 Response and Readiness and Online Learning initiatives. The Intel COVID-19 Response and Readiness Initiative will provide funding to accelerate customer and partner advances in diagnosis, treatment and vaccine development, leveraging technologies such as artificial intelligence (AI), high-performance computing and edge-to-cloud service delivery. Through the initiative, Intel will help healthcare and life sciences manufacturers increase the availability of technology and solutions used by hospitals to diagnose and treat COVID-19. It will also support the creation of industry alliances that accelerate worldwide capacity, capability and policy to respond to this and future pandemics, building on Intel's own experience in driving technology innovation in the health and life sciences arena.

The Intel Online Learning Initiative will support education-focused non-profit organisations and business partners to provide students, without access to technology, with devices and online learning resources. In close partnership with public school districts, the initiative will enable PC donations, online virtual resources, study-at-home guides and device connectivity assistance. The Intel Online Learning Initiative builds on Intel's long-standing commitment to technology that improves learning. It will begin immediately in regions with the greatest needs across the US and expand globally.

The company has also allocated up to USD 10 million for an innovation fund that supports requests from external partners and employee-led relief projects, addressing critical needs in their communities.

- Intel is working with India's Council of Scientific and Industrial Research and International Institute of Information Technology, Hyderabad, to deploy Intel client and server solutions to help achieve faster and less expensive COVID-19 testing and coronavirus genome sequencing to understand epidemiology and AI-based risk stratification for patients with comorbidities. Intel is collaborating with India's National Association of Software and Service Companies to build an application ecosystem and multicloud back-end to enable population scale COVID-19 diagnostics, predict outbreaks and improve medical care management and administration.
- Medical Informatics Corp's (MIC) Sickbay platform, powered by Intel technology, is a solution that can turn beds into virtual ICU beds in minutes, help protect critical care workers from risk of exposure with clinical distancing, and expand their care capacity significantly. Earlier, Houston Methodist Hospital deployed Sickbay for their vICU, and were able to leverage it within one day to support monitoring of its COVID-19 patients and enable their care providers to monitor patients virtually without risking exposure in their ICU rooms.
- In the UK, Intel is working with Dyson and medical consultancy firm TTP to supply FPGAs for CoVent, a new bed-mounted ventilator.

The objective

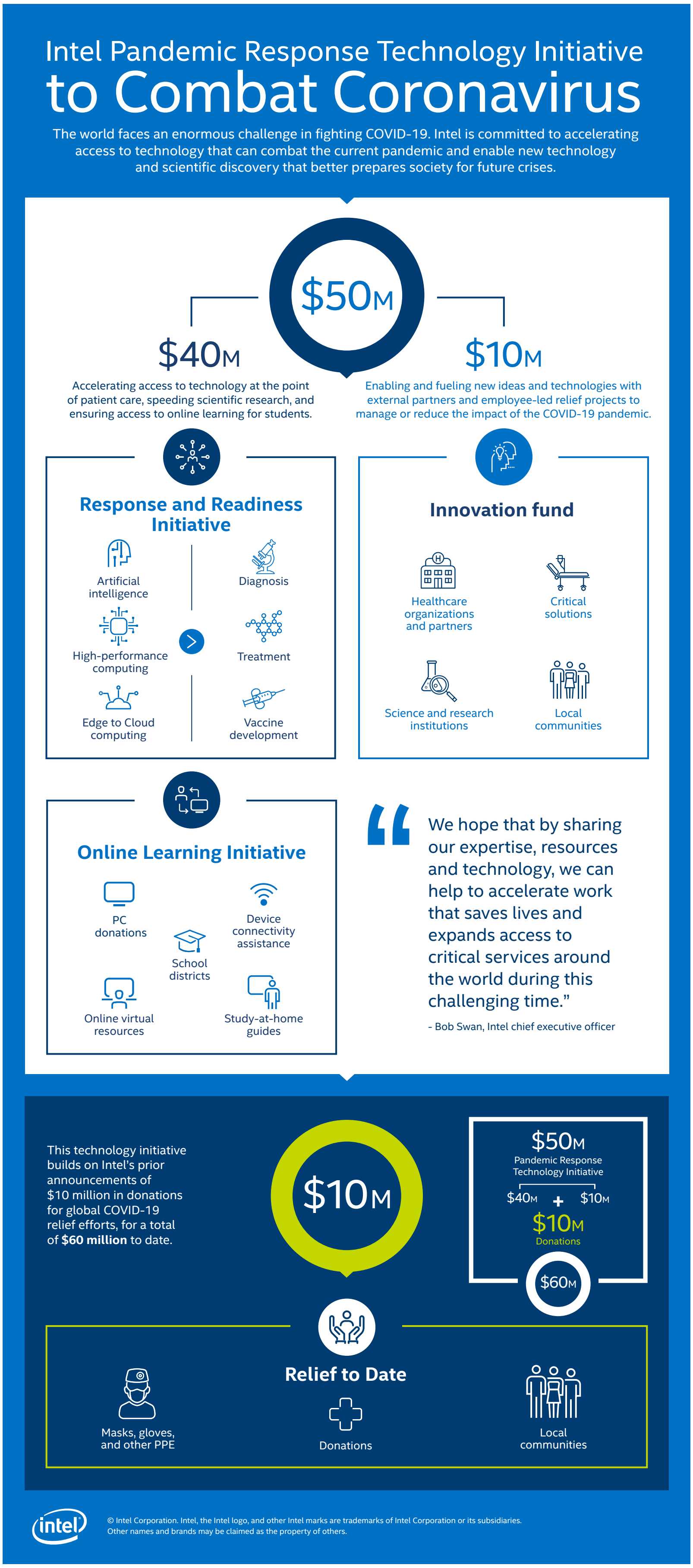
Intel technology underpins critical products and services that global communities, governments and healthcare organisations depend on every day. The company hopes that by harnessing its expertise, resources, technology and talents, it can help save and enrich lives by solving the world's greatest challenges through the creation and development of new technology-based innovations and approaches.

Coronavirus relief to-date

This technology response initiative builds on Intel's prior announcements of USD 10 million in donations that are supporting local communities during this critical time. Those donations include 1 million gloves, masks and other equipment for healthcare workers, USD 6 million from the Intel Foundation toward relief efforts in local communities and USD 4 million from Intel and its subsidiaries around the globe.

Additional technology efforts

As previously announced, Intel and Lenovo have teamed up with Beijing-based BGI Genomics to accelerate the analysis of the genomic characteristics of COVID-19. Intel has also joined the global XPRIZE Pandemic Alliance along with other companies to fuel collaboration on solutions through shared innovation to effectively address the immediate needs of the crisis.



Intel Pandemic Response Technology Initiative to Combat Coronavirus

The world faces an enormous challenge in fighting COVID-19. Intel is committed to accelerating access to technology that can combat the current pandemic and enable new technology and scientific discovery that better prepares society for future crises.

$50M

$40M

Accelerating access to technology at the point of patient care, speeding scientific research, and ensuring access to online learning for students.

$10M

Enabling and fueling new ideas and technologies with external partners and employee-led relief projects to manage or reduce the impact of the COVID-19 pandemic.

Response and Readiness Initiative

Innovation fund

Healthcare organizations and partners
Critical solutions
Science and research institutions
Local communities

Online Learning Initiative

> “We hope that by sharing our expertise, resources and technology, we can help to accelerate work that saves lives and expands access to critical services around the world during this challenging time.”
>
> - Bob Swan, Intel chief executive officer

This technology initiative builds on Intel's prior announcements of $10 million in donations for global COVID-19 relief efforts, for a total of **$60 million** to date.

Relief to Date

NI introduces new visual identity

National Instruments recently unveiled an updated brand identity including a new logo, visual identity, enhanced digital experiences and a brand campaign recognising and celebrating the contributions of engineers and enterprises who ‘Engineer Ambitiously’ every day. Now known simply as NI, the company is recommitting itself to connecting people, ideas and technologies required to push the world forward.

“At the heart of NI is our commitment to empowering engineers as they work to solve the problems of today, tomorrow and the next 100 years. Our customers are making their mark on the world. They inspire us all with feats of brilliance and innovations that will impact this planet and beyond”, said Carla Piñeyro Sublett, CMO at NI.

For more than four decades, NI has partnered talented engineers and enterprises using its test and measurement technologies to address some of the world’s most pressing challenges. From data and automation to research and validation, NI’s software-connected approach is helping its customers test new innovations quicker, more reliably and more safely. NI is modernising the test and measurement industry by coupling its rich software heritage with new cloud and machine learning capabilities to help customers rapidly create what is next.

INTRODUCING THE INFINIIUM MXR-SERIES OSCILLOSCOPE

The product combines the efficiency of an 8-in-1 bench solution with simultaneous 8-channel performance.

Keysight Technologies Inc, a leading technology company, announced the first oscilloscope with eight analog channels at 6 GHz and 16 simultaneous digital channels, enabling customers to reduce test bench and workflow complexity to achieve higher performance as well as accurate and repeatable multi-channel measurements in a single instrument.

High-speed digital designs, power integrity verification, Wi-Fi 6, IoT, IIoT and imaging, and Gallium nitride (GaN) semiconductors utilise frequencies between 2 GHz and 6 GHz, that are currently underserved or require costly trade-offs. Testing these new products requires time- and frequency-domain equipment capable of simultaneous analog and digital channels, ideally with software enabled protocols, standards, built-in test assistance, and remote collaboration with the test team.

The new Infiniium MXR-Series mixed signal oscilloscope offers advanced ASIC-driven processing, resulting in eight powerful instruments in one, including a real-time spectrum analyser (RTSA), oscilloscope, digital voltmeter (DVM), waveform generator, Bode plotter, counter, protocol analyser, and logic analyser. It is complemented by an extensive suite of software solutions focused on power integrity, high-speed digital testing and verification. Built-in software includes a fault hunter function that speeds root cause identification and resolution of rare or randomly occurring errors.

The Keysight Infiniium MXR-Series oscilloscope helps engineers get from symptom to resolution quickly, with the following key customer benefits:

- Eight powerful instruments in one reduces bench clutter, setup and test time, while minimising crosstalk issues. Incorporating a real-time spectrum analyser achieves a 100% probability of detection in the frequency domain, even for asynchronous errors.
- A built-in fault hunter function learns normal signals and compares them over time, to find abnormal signals, capturing everything else that occurs when the abnormal signals are produced. This results in rapid problem resolution for troubleshooting irregular, random or spurious signals.
- Simultaneous eight analog channels and 16 digital channels enable monitoring and analysis of complex signal interactions. Coupled with 3X higher bandwidth than any other eight-channel oscilloscope, it allows test engineers to open a wider and more insightful window into designs.
- Powerful remote collaboration with PathWave Infiniium Offline Analysis software enables design teams to do extensive analysis and data manipulation after bench measurements are complete, enhancing the efficiency and effectiveness of the test bench.

"The Infiniium MXR-Series benefits from a unique combination of Keysight's technology and solution expertise", said Mr Lawrence Liu, General Manager for Asia Pacific, Keysight Technologies.

"This innovative family joins Keysight's portfolio of oscilloscope solutions - a portfolio that addresses a wide range of application requirements - from low to very high frequencies, economical to high performance, and foundational measurements to advanced analysis and visualisation", he added.

Keysight Technologies

Solutions from Keysight Technologies optimise networks and bring electronic products to market faster and at a lower cost, with offerings from design simulation, to prototype validation, to manufacturing tests, and to optimisation in networks and cloud environments. Customers span the worldwide communications ecosystem, aerospace and defence, automotive, energy, semiconductor and general electronics end-markets.

Keysight Infiniium MXR-Series, 8 channel, 6 GHz oscilloscope with (clockwise, from top left) US FM radio, 2.4 GHz WLAN, 5 GHz WLAN, and Bluetooth displayed in RTSA mode.

Benefits for a range of users

Mr Lawrence Liu, General Manager for Asia Pacific, Keysight Technologies provides more information on the advantages of, and the areas of application for, the new MXR-Series Mixed Signal Oscilloscope.

'The Singapore Engineer': What are some of the features of the Infiniium MXR-Series of products?

Mr Lawrence Liu, General Manager for Asia Pacific, Keysight Technologies.

Mr Lawrence Liu: The Infiniium MXR-Series mixed-signal oscilloscope is the world's first and only oscilloscope with eight analog channels at 6 GHz, and 16 simultaneous digital channels. Its state-of-the-art ASIC-driven processing enables eight powerful instruments in one.

The Infiniium MXR-Series is complemented by an extensive suite of software solutions focused on power integrity and high-speed digital testing and verification. Its software is backwards-compatible so that designers can use previously created code. Built-in software includes a fault hunter function that speeds root cause identification and resolution of the most challenging, rare or randomly occurring errors.

The Infiniium MXR-Series joins the Infiniium family of products, including the S-Series, V-Series, Z-Series, and the world's highest performance oscilloscope - the UXR-Series. It expands the portfolio with greater multi-channel capabilities to support demanding new industry applications. The entire Infiniium product line also includes unmatched remote collaboration capabilities that enable a vastly improved test workflow.

Q: How will the new series assist users?

A: The MXR Series will help customers reduce their test bench and workflow complexity and achieve higher performance as well as accurate and repeatable multi-channel measurements in a single instrument.

Keysight Infiniium MXR-Series, 8 channel, 6 GHz oscilloscope performing DDR measurements and analysis.

The Infiniium MXR-Series helps designers work with higher bandwidth signals simultaneously across more analog and digital channels than ever before. This opens up additional product families for test, such as Wi-Fi 6, higher frequency IoT, 5G FR1, and massive Multiple Input Multiple Output (MIMO) products, that were beyond the capability of previous oscilloscopes in this class.

Reduced troubleshooting time for random errors and dramatically improved test workflow enhanced by remote team collaboration complement the higher performance to get engineers from symptom to root cause to solution faster.

Q: What are the target industrial sectors for the new oscilloscopes?

A: Key customers that we are targeting include enterprises in the semiconductor, circuit board and subsystem, consumer electronics, medical device, telco & IoT devices, network, data centre, system architecture and integration, auto electronic, general electronic, 3D component design, and education fields.

Q: And some of the specific areas of application?

A: In terms of industry applications, the Infiniium MXR-Series supports the following:

- Wi-Fi 6: Thoroughly testing the new generation of Wi-Fi 6 devices requires simultaneous channels due to complex hardware along with deeper insights into the effects of power supply switching and noise. AX is coming fast in an array of new devices. The critical spectrum between 2 GHz and 6 GHz is where all that critical testing will be done.
- IoT: Wi-Fi 6 allows for higher density of devices, opening the door to many users per node than previous generation sharing ever could. The resulting applications for the industrial and consumer internet of things bring countless new opportunities. 5G expands Wi-Fi 6 farther afield. Testing needs for 5G FR1 integrated with Wi-Fi 6 demand more channels simultaneously in the 2 GHz to 6 GHz spectrum.
- Semiconductors: Sub 6 Ghz massive MIMO technology will solve many of today's interference problems by using many antennas at the base station. The requirement for much higher power output and higher frequencies will increasingly bring Gallium nitride (GaN) semiconductor technology into play. GaN semiconductors' smaller packaging demands new testing approaches that monitor crosstalk simultaneously across multiple channels.

GEARING UP FOR GROWTH:

TACKLING CHANGE HEAD-ON

by Vincent Tang, Regional Vice President, Asia, Epicor

Major aspects of the ‘smart factory’ are presented.

Mr Vincent Tang

The changing nature of products and customer engagement in manufacturing is creating new industry segments and re-inventing, sometimes even eliminating, others. In this ever-changing environment, manufacturers need to be aware of the risks of being left behind if they do not master emerging technologies.

But manufacturers need a compelling reason based on business gains and/or competitive pressures in their markets to make this change. Any shift in practices and processes has traditionally been slow, and expensive, with often disastrous results if not approached in the right way.

So why should companies start investing in, for example, ‘smart factory’ technologies now? The answer is that they need to do this to ensure future survival and to capitalise on growth opportunities.

In a survey conducted by Morar Consulting, on behalf of Epicor, in December 2017, 50% of the respondents said they believe strongly that they have the tools to grow, but 29% are unsure where that growth will come from. The research questioned 2,200 decision-makers and employees in manufacturing businesses in 14 countries across the globe.

To help manufacturers follow the right path, let us take a look at some of the areas that have high potential for growth.

Personalisation

The need for instant gratification and personalisation is pushing product engineering and manufacturing to new levels of complexity. What customers want from products, how they want to consume them and what relationship they have with the manufacturers who produce them, are all changing.

To maintain costs and product quality, manufacturers must increase their effectiveness by learning to combine factory automation with process flexibility. In the smart factory, processes need to go beyond automation and become autonomous. The smart factory deploys intelligent machines that will help make decisions in more flexible and unstructured ways.

Evolution of factory intelligence

Many emerging technologies will be deployed to help create these enhanced capabilities. Artificial intelligence will develop so that it transforms our current understanding of product configuration, production scheduling, and real-time decision-making, for optimised profitability. Data generated from and shared with other smart machines turns into intelligence that ensures that manufacturing assets operate as a balanced system. The need for embedded analytics and manufacturing intelligence across the factory floor and beyond is a necessity for manufacturers trying to optimise and improve processes and productivity.

Product innovation

The digitisation of the economy is also changing the nature of product development. Data will no longer be a by-product of the manufacturing process, but will deliver increasingly important insights both for the customer and manufacturer. Physical, digital, and social capabilities become parts of the same product, inevitably increasing the complexity of product design, new systems and collaboration with ecosystem partners.

A hyper-connected business

The exponential adoption of advanced technologies presents a vast array of potential changes and investment demands for manufacturing in the years ahead. Huge datasets, AI and autonomous production will combine to execute complexity that extends beyond the human capacity to manage in real-time. A virtual facsimile of the physical factory will become the interface to production as physical execution becomes increasingly removed from direct human management decisions and intervention.

The future is here

The smart factories of the near future have already begun their digital transformation and early adopters are beginning to create a competitive advantage. By investing in emerging technology, companies are creating technical expertise and the critical digital transformation culture they need, to succeed and thrive in the years ahead.

Underpinning this fundamental change in factory processes is enterprise resource planning (ERP) solutions. No amount of automation or innovation will succeed without a way to effectively manage the change or have clear visibility of where efficiencies can be made, and the true value realised. Only then will manufacturers reap the benefits of the current and future waves of technological advances.

BOOSTING INNOVATION IN DIGITAL DESIGN

AND ADVANCED MANUFACTURING

Two organisations deepen R&D collaboration.

Sembcorp Marine and the Agency for Science, Technology and Research (A*STAR) have signed a Master Research Collaboration Agreement (MRCA) to jointly pursue innovation in digital design and advanced manufacturing. With this agreement, the partners aim to shorten the development cycle and time-to-market of new offshore, marine and clean energy solutions achieved through their research efforts.

Under the MRCA, Sembcorp Marine and A*STAR will set up Joint Lab@TBY, a research laboratory and work space at Sembcorp Marine Tuas Boulevard Yard, that will facilitate the test-bedding and commercialisation of new digital design solutions, advanced manufacturing capabilities and other Industry 4.0-related technologies in a real-world environment.

Digital design solutions to be explored include novel designs that support the development of offshore wind energy and risk mitigations in liquefied natural gas (LNG) storage and transportation.

Joint Lab@TBY also seeks to augment local advanced manufacturing capabilities in the following areas:

- Large format additive manufacturing technology.
- Automated robotic welding for complex offshore structures.
- Automated non-destructive testing (NDT).
- Smart factory floor monitoring and control.

Speaking at the MRCA signing ceremony earlier this year, Sembcorp Marine President and CEO Mr Wong Weng Sun said the partnership with A*STAR will greatly enrich Sembcorp Marine's efforts to develop cutting-edge, cost-competitive and greener engineering solutions.

Mr Wong said, "Innovation is a core enabler at Sembcorp Marine and we are constantly looking at new ways to boost our engineering capabilities, production capacity and efficiency. Given the rapid technological disruption and rising environmental consciousness in the global markets, we must continuously push the innovation envelope and deliver sustainable solutions that keep us relevant to our customers. Partnering a top-class research organisation like A*STAR will help Sembcorp Marine achieve these vital objectives and stay ahead of the technology curve".

Mr Wong said Tuas Boulevard Yard, with its operations and ongoing construction projects, will provide Sembcorp Marine and A*STAR researchers a real-world environment to experiment, test-bed and validate new technologies.

sembcorp marine
Agency for Science, Technology and Research SINGAPORE
Master Research Collaboration Agreement Signing Ceremon
DIGITAL DESIGN AND ADVANCED MANUFACTURI
ebruary 202

*At the MRCA signing ceremony are, from left to right, Mr Wong Weng Sun, President & CEO, Sembcorp Marine; Mr Simon Kuik, Head of R&D, Sembcorp Marine; Professor Tan Sze Wee, Assistant Chief Executive, Science and Engineering Research Council, A*STAR; and Mr Frederick Chew, CEO, A*STAR.*

"In this conducive environment, we are confident the Joint Lab@TBY team can deliver effective digital design and advanced manufacturing solutions fruitfully", he said.

Since 2013, Sembcorp Marine, A*STAR and various other stakeholders have been working together on research projects such as green shipping and workshop automation, under individual agreements. The MRCA allows Sembcorp Marine to team up with multiple A*STAR research entities under a common framework. This arrangement will smoothen the execution of future R&D collaborations, attract participation from more organisations, and enable the cross-fertilisation of unique insights and ideas to create impactful solutions.

Mr Wong added, "Sembcorp Marine views the MRCA not only as a natural progression of our long-standing working relationship with A*STAR, but also as an example of how the public and private sectors can work with each other towards highly rewarding research outcomes. We are honoured to have A*STAR on board our R&D journey".

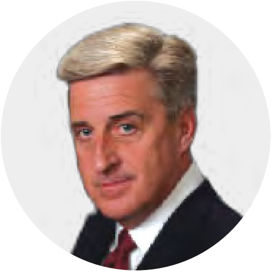
Mr Frederick Chew, Chief Executive Officer of A*STAR, said, "A*STAR is committed to strengthen support for local enterprises such as Sembcorp Marine, one of the key players in Singapore's Offshore and Marine ecosystem. Sembcorp Marine is a long-time partner, and our collaborations have led to positive outcomes for industry and the economy. This MRCA to co-innovate in digital design and advanced manufacturing takes our partnership to a new level".

Recent projects between Sembcorp Marine and A*STAR included the development of 3D printing and Industrial Internet of Things (IIoT). Sembcorp Marine and A*STAR have also embarked on projects in optimising engineering designs for gas hybrid tugs, gas containment systems and performance-based assessment for gas leaks and dispersion.

HOW TO MANAGE MAJOR DISRUPTIONS IN THE SUPPLY CHAIN

by Greg Smith, Managing Director, Americas, Proudfoot

A specialist in operational management and digital transformation addresses the current situation and offers practical solutions.



Mr Greg Smith

The worldwide COVID-19 pandemic has exposed glaring vulnerabilities in today's global supply chains, making it essential for businesses to quickly and effectively develop risk management plans for their supply chains.

Despite the last decade seeing several catastrophic events, including the disastrous hurricanes that hit the US, Puerto Rico and the Virgin Islands in 2017, Japan's 2011 devastating tsunami, and 2010's volcanic eruptions in Iceland that grounded flights worldwide, most companies were still underprepared for the COVID-19 pandemic.

THE CHINA VARIABLE

With a vast majority of the global supply chain moving through China, it is essential to acknowledge how much Chinese firms have improved their operations over the years. They have increased capacity and output exponentially, built increasingly complex products domestically and streamlined downstream processes in domestic transport, sea freight, unloading and customs clearance, to reduce risk and administration.

On the flip side, China has introduced relatively high labour inflation for over 10 years, and this has eroded cost benefit over time. Indeed, some European automotive component manufacturers, have moved operations from China to more competitive labour markets in Turkey and North Africa.

Additionally, firms that do business in China frequently fail to increase the inventory of safety stock, instead of making a trade-off for cash. When operations in China unexpectedly ground to a halt, as we witnessed earlier this year, this failure adds more risks to an already dysfunctional supply chain.

THE CASE FOR SUPPLY CHAIN RISK MODELLING

The supply chain was much simpler when companies started sourcing in China. Today, the supply chain is increasingly complex, fuelling the need for a supply chain risk model. Without it, companies are unable to manage the current fragility of the global business landscape efficiently.

Companies must consider every link in the supply chain, as well as risks associated with each link. Natural disasters, regional economic instability, and other potential disruptions can result in delays, higher costs, lower sales and customer dissatisfaction.

The COVID-19 pandemic was unprecedented on the levels of global disruptions triggered. It may go down in history as a black swan event. Still, it also crystallised the need for well-defined and easily deployable supply chain risk management plans to businesses worldwide.

CREATING A SUPPLY CHAIN RISK MANAGEMENT PLAN

In today's global business world, there are many unpredictable events impacting supply chains. Leaders must bulletproof their supply chains and strategically think ahead to mitigate risks.

Proudfoot has compiled the following five-step, high-level overview of how to start thinking about supply chain risk management plans (SCRMPs) that will protect businesses against disruptions in the supply chain:

Locate the risks

The first step in disaster planning is mapping out every critical facet of the supply chain exposed to risk. Consider risk locations such as partner suppliers, production lines, procurement processes, transportation providers, warehousing and technology.

Specific risks can be determined based on geography, climate, or socio-political events. General risks include cybersecurity and changing industry trends. For companies without an integrated SCRMP, the priority should be identifying such risks and designing operational data-driven strategies to mitigate them. By questioning the likelihood of these risks and their impact, organisations can save costs and ensure timely deliveries to maintain customer satisfaction and profit margins.

Quantify the risks

Some risks cause minor interruptions while other risks could spell disaster. Rate each risk in terms of likelihood and severity. By assigning a rating, risk management teams can predict the threat of each risk. One such method to quantify risk is the Failure Mode and Effect Analysis (FMEA). Organisations can then identify risks that need immediate attention and prioritise other risks according to their rating on the scale.

Build contingencies

By building 'what if' scenarios, companies can determine the response to each event if it were to happen. Risk teams are responsible for developing detailed strategies to navigate specific risks such as delays, tariffs, product recalls and natural disasters. Alternative options for sourcing are critical to be contingency-efficient.

Build the plan

Once you assess the risks, model the scenarios, and document the responses, teams can construct an actionable SCRMP. They include the following steps:

- Integrate industry best practices for supply chain risk management.
- Create a detailed value proposition.
- Meet experts to identify potential supply chain risks before and after production.
- Identify a dedicated project manager or risk manager to generate ideas, take ownership of individual risks and delegate responsibilities.

Actionable deliverables in a plan include making a list of qualified alternative suppliers by region, pricing and other risk constraints. Ideally, leaders should review their plans regularly, as volatile business environments can rapidly lead to negative consequences.

Insure the supply chain

There are two types of insurance policies. Formal insurance policies and insurance that comes from developing the right approaches to mitigate risk.

Formal insurance

A good insurance policy can complement a fool-proof SCRMP. A recent study found that insurance policies were the least common mitigation strategy among surveyed companies. Supply chain experts now see potential value in insurance to recoup costs in significant disruption.

Insurance companies specialise in risk management. They can also help to build proper contingency plans. Some policies provide coverage for production lines and equipment damages. Others cover upstream occurrences, such as delays of parts from overseas suppliers. Insurance may not fully cover losses, but it can soften the blow by recouping some costs and recovering from losses.

Right-execution and right-partner insurance

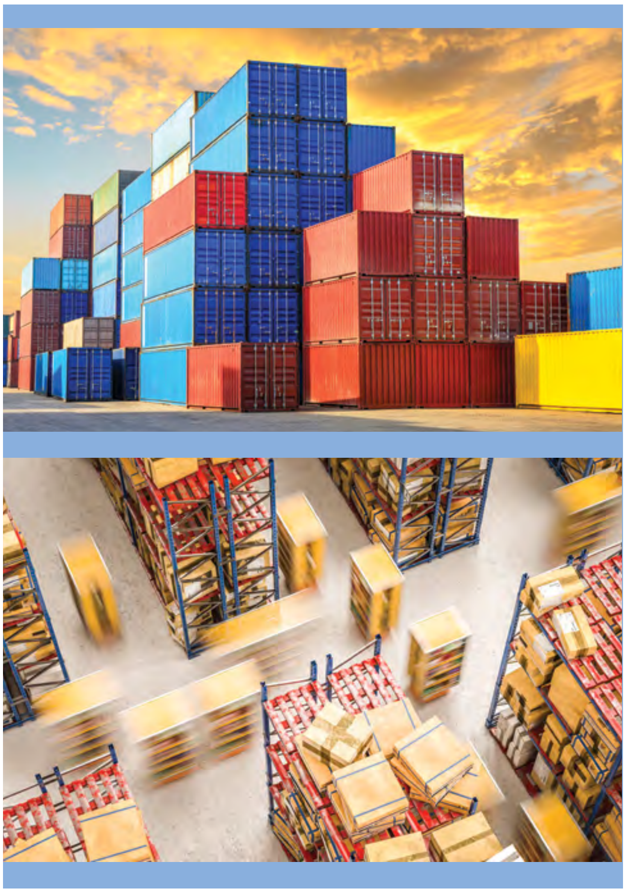
A risk-centric journey implies a holistic transformation of the way a change is approached, executed, embedded and sustained in the organisation. Formally insuring operations and developing a SCRMP is important. However, a clear, deliberate, expertly designed and accelerated execution of a transformation plan that focuses on objectives and priorities, assessment of likely risk impact on the current operating model, and develops a well-sequenced transformation roadmap, might prove to be the differentiator between companies that survive future supply chain risks and those that do not. The transformation roadmap must take into account all stakeholders, constraints, behaviours, communications and financial implications.

The path toward a robust SCRMP

In today's hyper-competitive marketplace fraught with risks, there is little margin for error. A debilitating supply chain leads to significant business losses and competitors can quickly grab potential market shares.

Businesses can transform positively by implementing the right change management strategies and with the right insurance partners. With clearly defined objectives, risk assessments and priorities, companies can develop a transformation roadmap with stakeholders and costs in mind.

While designing and reviewing an SCRMP is essential, it is imperative that organisations execute them quickly and effectively. Day-to-day operations can easily derail the SCRMP if they are not implemented promptly with the right governance. Having the right partnerships and execution strategy is critical to a robust SCRMP.



The worldwide COVID-19 pandemic has exposed glaring vulnerabilities in today's global supply chains.

THE SPRAWLING REACH OF COMPLEX THREATS

Trend Micro Incorporated, a global leader in cybersecurity solutions, recently released its 2019 Annual Security Roundup Report. 'The Singapore Engineer' presents, in two parts, edited contents of the report. Below is the first part.

INTRODUCTION

The 2010s saw a shift in the cybersecurity industry, as well as much of the rest of the IT landscape, from on-premise to cloud. This progression was occasioned by innovations in various technologies and in the ways the industry had adapted to a great many changes in the landscape. Unfortunately, it was also mirrored by the evolution of cyber threats which had gone a long way from basic and intermittent to complex and persistent. A testament to this was the high-profile threats that made their mark in the security landscape of the last year of the decade, which were notably diverse in terms of the entities and platforms they affected.

Ransomware operators zeroed in on government organisations, and deployed attacks that exhibited technical efficiency and were laced with next-level intimidation tactics. A popular office suite became even more favoured among phishers, and cyberespionage campaigns showed an increasing inclination towards compromising mobile devices.

Vulnerabilities continued to set the alarm bells ringing, most blaringly with the disclosure of a 'wormable' flaw in a widely used software protocol. In addition, the internet of things (IoT) remained fertile ground for botnets that exploited old and known weaknesses.

Supply chain attacks were in the spotlight, thanks mainly to a notorious consortium of hacking groups that targeted e-commerce websites. Threats to software development tools and platforms, particularly those associated with the collaborative approach known as DevOps, became more prominent. And detection-evading 'fileless' threats ironically made their presence more felt in the cases of different systems and platforms hit by malware that incorporated them.

Already, enterprises are faced with the challenging tasks of integrating and maintaining cloud, IoT, mobile, and other technologies into their infrastructures. But there is another task that enterprises would do well not to give short shrift to - that of securing their infrastructures at all layers, especially since the landscape is becoming increasingly riddled with complex and persistent threats that could have an impact on their operations, reputations, and bottom lines.

Our latest annual security roundup takes a deep dive into the most important issues that shaped the threat landscape of 2019, thereby providing enterprises with insights into the best practices and strategies for protecting their infrastructures from current and emerging threats.

Ransomware homes in on particular targets

Targeted ransomware plagues government sector

In 2019, ransomware operators' shift to a more targeted approach allowed them to orchestrate attacks where organisations' critical assets, systems, and services were sought after and compromised to bountiful effect. This shift in strategy involved novel attack techniques that enabled them to perform actions such as swiftly moving laterally into the network and deploying as many pieces of malware as possible. One of the more notable techniques operators used in the past year involved compromising rarely targeted resources, such as domain controllers and active directories, in order to cause bigger disruptions and subsequently force affected organisations to give in to their demands.

The effectiveness of the overall shift in strategy was tested and proved in ransomware attacks on the government sector, which became something of a global phenomenon in 2019. This trend was particularly prominent in the US, where a number of high-profile ransomware attacks on government entities occurred.

In April, the US Virgin Islands Police Department was hit by a ransomware attack that encrypted internal affairs records and citizen complaints. In August, the city of Lodi, California, suffered from an attack that compromised its financial systems and critical phone lines.

An incident involving the city of Pensacola, Florida, shone a light on a tactic not historically seen in previous ransomware cases. After compromising the city's email and phone services, the group behind the attack, known as Maze, deliberately released 2 GB of the 32 GB of stolen files to prove that it had in fact gotten a hold of the city's data besides encrypting the network. Maze had already leaked stolen data after its other victim organisations missed ransom payment deadlines. In the case of Pensacola, however, the group maintained that it made the move not to pressure city officials into paying the USD 1 million ransom it had been asking, but merely to counter the media's claim that it had been stealing data of just a few files.

The success of Maze's attack could be attributed to the capability of the deployed ransomware, also called Maze, to automatically copy all affected files to servers controlled by its operators. This capability results in an additional burden to victim entities. Not only would they have to deal with data encryption, but they would also have to reckon with the aftermath of a data breach.

Valuable insights to deal with cyber threats

The Trend Micro 2019 Annual Security Roundup Report details the most important issues and changes in the threat landscape, to provide businesses with insights into best practices and strategies for protecting their infrastructures from current and emerging threats.

Ransomware continued to be a mainstay cyber threat last year. Overall, Trend Micro discovered a 10% increase in ransomware detections, despite a 57% decrease in the number of new ransomware families.

The modus operandi morphed in 2019. Trend Micro saw ransomware increasingly becoming a secondary infection vector and alliances being forged to carry out an elaborate, complex ransomware scheme. Under the partnership, one group gains access to a network, and sells the access to another group to execute a ransomware attack. This shows that groups are becoming more specialised and are segmenting the pieces of a cybercriminal business model.

The report also revealed that email remained the top threat vector used by cybercriminals in 2019. Globally, Trend Micro blocked 15% more email threats in 2019 than in 2018. This pattern held true in Singapore. Trend Micro blocked more than 413 million email threats in the city-state, a 19.9% increase from 2018.

Phishing continued to be the top threat to organisations in 2019 and started to feature advanced techniques. As a result, such threats targeting Office 365 increased two-fold. Business email compromise (BEC) is a notorious form of phishing attack. It grew by 5% last year. A global trend observed by Trend Micro showed BEC operators expanding from their traditional enterprise victims to encompass religious, educational, and non-profit organisations.

Further 2019 Singapore findings

- Trend Micro recorded a 54.5% year-on-year decline in the number of times it blocked malicious URLs hosted in Singapore. This is the number of times Singapore-hosted malicious URLs are being accessed by users across the globe.
- On the flipside, the number of times users in Singapore accessed malicious links (which is the number of times malicious URLs hosted anywhere in the world, including Singapore, are being accessed by users in Singapore), rose by 32.5%, compared to 2018 - pointing towards the need to empower users to identify risks through education.

"Our 2019 findings revealed how cybercriminals recognised the high return on investment from ransomware and BEC scams - a single successful attempt could make for a lucrative yield, even factoring in the research and other efforts that went behind it", said Mr Nilesh Jain, Vice President, Southeast Asia and India, Trend Micro.

Mr Nilesh Jain

"The traditional approach of using numerous best-of-breed security solutions is not today's state-of-the-art security. As the security stack becomes bloated, efficiencies need to be identified and had. By the end of the day, having 20 security solutions that do not talk to each other at all, may not be as effective as having five that do", he added.

Known vulnerabilities remain key to successful cyber attacks, including ransomware. In 2019, Trend Micro's Zero Day Initiative (ZDI) disclosed 171% more high severity vulnerabilities than in 2018. The criticality score reflects the likelihood of these flaws being leveraged by attackers, so high severity bugs are more likely to be weaponised and the patches should be prioritised.

To protect against today's threat landscape, Trend Micro recommends a connected threat defence across gateways, networks, servers and endpoints. Additionally, the following best practices can increase a company's security posture:

- Mitigate ransomware with network segmentation, regular back-ups and continuous network monitoring.
- Update and patch systems and software to protect against known vulnerabilities.
- Enable virtual patching, especially for operating systems that are no longer supported by the vendor.
- Implement multi-factor authentication and least privilege access policies to prevent abuse of tools that can be accessed via admin credentials, like remote desktop protocol, PowerShell and developer tools.

More information on the cyber threat landscape of 2019 can be obtained by accessing the full report via the following link: https://www.trendmicro.com/vinfo/sg/security/research-and-analysis/threat-reports/roundup/the-sprawling-reach-of-complex-threats.

Security experts have remarked on the effect this could have on the implementation of incident response in organisations, which could mean the IT department would now have to coordinate with legal and other departments to plan additional recovery steps.

Another important development seen in 2019 was the formation of alliances between ransomware groups, including at least two that targeted US government organisations, and 'access-as-a-service' providers, or entities that rent out or sell access to different company networks. The latter, which rely on network intrusion experts, price their services from USD 3,000 to USD 20,000, with their most expensive 'package' including full access to a company's administrative panel, server hosts, and virtual private networks (VPNs).

The operators behind Ryuk, who launched a ransomware attack on the Office of Technology Services of Louisiana in November, were believed to have been working with access-as-a-service providers. They reportedly had been renting access-as-a-service malware such as Trickbot to gain unauthorised entry into systems of organisations whose networks had been infected with the malware. Another group that is infamous for working with access-as-a-service providers is the one behind the Sodinokibi ransomware, aka Sodin or REvil. In August, the operators of Sodinokibi launched coordinated attacks on 22 local government units in Texas, demanding a combined USD 2.5 million ransom. The ransomware was said to have been deployed through compromised third-party software that was shared by the victim municipalities.

At least 110 state and municipal governments and agencies in the US fell victim to ransomware attacks in 2019. Despite the unprecedented spate of attacks on government entities, however, the healthcare sector remained the top ransomware target in the US, with more than 700 healthcare providers affected by ransomware in the past year. The US education sector was not far behind the government sector, with over 80 universities, colleges, and school districts hit. Ransomware operators target the healthcare, government, and education sectors because the damage they could exact extends beyond the victim organisations. Concerned individuals would also be affected since these sectors provide services that are essential to them. These sectors cannot afford to have their services taken offline or otherwise disrupted because of the far-reaching consequences.

Insurance coverage gains more prominent role in ransomware payouts

It could be surmised that ransomware operators increasingly targeted the government sector in 2019 because of the willingness of many victim organisations to pay the ransom. This trend could be a progression from previous attacks in the private sector where victim companies had shown a propensity to pay ransomware operators. In 2017, for example, about half of victim companies in the US reportedly paid at least one ransom. In their desire to cut losses from the disruption of their operations, victim organisations would rather negotiate with and subsequently pay ransomware operators than ignore their demands.

In July, the government of LaPorte County, Indiana, found its systems paralysed by ransomware whose operators had demanded USD 250,000. It agreed to pay USD 132,000 instead, USD 100,000 of which was covered by its insurance provider. The county commission's president called the move an 'economic decision', meant to curtail the time necessary to restore operations. In the same month, the city of New Bedford, Massachusetts, offered to pay attackers who had locked up its computers only USD 400,000 instead of the USD 5.3 million that they had asked for. The city mayor later revealed that while he was initially hesitant to offer payment, it would have been remiss of him not to consider the possibility of receiving the decryption key if the full cost of the ransom could be covered by the insurance provider.

Evidently, insurance providers' coverage of a large portion of the payouts in ransomware attacks helps expedite the recovery of encrypted data and disabled systems. But victim organisations' increasing reliance on it is concerning in that it encourages cybercriminals to target more entities that may have insurance coverage.

No less than the FBI remained firm on its stance against paying ransom. In September, the agency's Cyber Section chief advised victims to refuse paying ransomware operators because doing so does not guarantee that their data and systems will be restored. In one example he cited, a ransomware victim paid the operators in hopes of receiving a decryption key, but the key that was provided erased all of the victim's data.

Notable ones emerge among relatively few new ransomware families

There was an uptick in our detections of ransomware-related threats (files, emails, and URLs) in 2019. The slight increase could be reflective not only of our proactive blocking of ransomware-related activities at the email and URL layers, but also of an overall improvement in security mechanisms that blocked ransomware past its download stage.

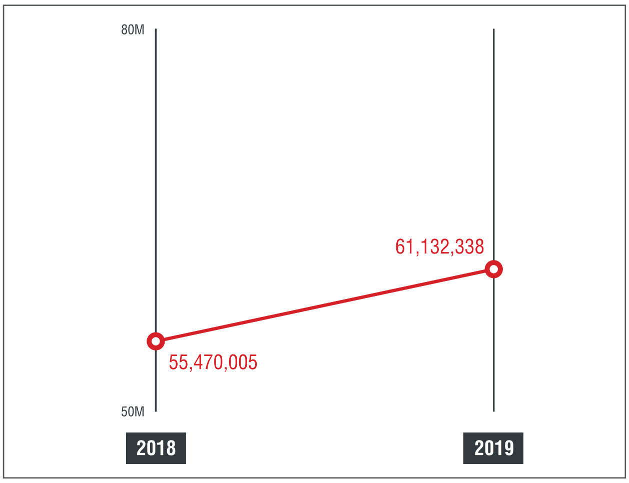


Figure 1: Ransomware-related threat components (files, emails, URLs) slightly increased: Year- on-year comparison of the number of detections of ransomware-related threats. Source: Trend Micro Smart Protection Network infrastructure.

The number of new ransomware families continued to decline from year to year, with just under a hundred detected in 2019 - fewer than half of the corresponding count in 2018. This could mean that threat actors had found a firmer footing in selective targeting than in creating new forms of ransomware.

Nevertheless, threat actors were able to spawn new ransomware families that can be considered impactful and notable in their technical capabilities. One of these was the Snatch ransomware, which was first spotted in October and had been used in attacks on organisations in the US, Canada, and several countries in Europe. Snatch can force Windows machines to reboot into safe mode in order to bypass security software and encrypt files without being detected. This capability was crafted to take advantage of some security software that does not run in safe mode, which is meant for recovering a corrupt operating system and debugging.

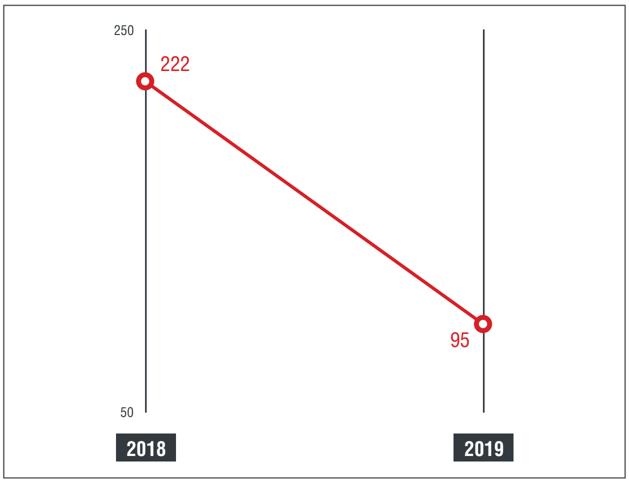


Figure 2: New ransomware families declined: Year-on-year comparison of the number of detections of new ransomware families. Sources: Trend Micro Smart Protection Network infrastructure and analysis of externally sourced data.

Another new ransomware family of note was Zeppelin, which was first seen with compilation timestamps of no earlier than November and observed infecting companies in the US and Europe. Samples of Zeppelin showed that it is highly configurable and can be deployed as a .dll or .exe file, or wrapped in a PowerShell loader. Aside from encrypting files, it is capable of terminating various processes. And its ransom notes have different versions, varying from generic messages to longer ones customised to its target organisations.

Another new family that stood out was the aforementioned Maze ransomware, which can automatically copy all affected files to operator-controlled servers. The eponymous group behind Maze also used fake cryptocurrency sites, malicious spam campaigns, and even exploit kits to breach a network. Maze's successful breach of its targets' networks has earned its operators a reputation for releasing stolen data if their victims decline or fail to meet their monetary demands.

Messaging threats remain viable for attackers

Phishing threats to Office 365 increase twofold

Phishing was the top threat to organisations in 2019, according to our latest Cyber Risk Index study, which surveyed more than a thousand organisations in the US. But while phishing persisted in the past year, our detections of activities related to it dropped from the previous year. The instances of blocked access to non-unique phishing-related URLs decreased by 28% from 2018. And the number of users who would have been affected by phishing-related sites also declined. The instances of blocked access to phishing URLs by unique client IP address decreased by 38% from the previous year. The growing number of enterprise users of newer messaging platforms such as Slack as alternatives to email might have contributed to the drop in detections.

Ransomware family	How it can arrive and attack vectors used	How it can propagate	Notable characteristic
Maze	Malicious spam, fake cryptocurrency websites, exploit kits	Compromised software, compromised frameworks (e.g., PowerShell), other malware variants	Exfiltrates files before encrypting machines and network shares
Snatch	Exposed remote desktop ports	Compromised remote desktop services, domain controllers, compromised legitimate tools (e.g., PsExec)	Reboots infected machines into safe mode to evade detection
Zeppelin	Compromised remote desktop control tools, malvertisements, compromised websites	Compromised frameworks (e.g., PowerShell)	Wraps its executables in three layers of obfuscation
LockerGoga	Compromised credentials, compromised active directories	System administration and possibly penetration testing and other hacking tools, valid certificates to evade detection and get into systems	Modifies passwords of infected systems' user accounts, prevents infected systems from being rebooted
Clop (CryptoMix)	Compromised active directories	Compromised remote desktop services	Uses executables with a valid digital signature for distribution

Table 1: Notable new ransomware families used varying and technically efficient methods: Comparison of the routines of notable ransomware families that emerged in 2019.

Despite the decrease in overall phishing activities, phishing URLs that spoofed Microsoft Office 365, particularly Outlook, continued on an upward trend. The number of blocked unique Office 365-related phishing URLs in 2019 doubled from the previous year.

The widespread adoption of Office 365, which reached the 200 million monthly active users milestone in October, is one reason for its sustained popularity as a prime target among cybercriminals. Another is the value of Office 365 accounts for spamming: Cybercriminals are inclined to abuse the Microsoft email architecture, which also includes Hotmail, Live Mail, and MSN Mail, because phishing emails coming from Microsoft's email services are likely whitelisted or are more difficult for security solutions to block. In addition, a compromised Office 365 account could allow a cybercriminal to conduct internal phishing attacks in an organisation without needing to spoof an email address, making it harder to spot the attacks.

Phishing scams pull new tricks

Cybercriminals had been continually refining their techniques to improve their chances of deceiving users of messaging tools such as email and SMS. This much was indicated by the advanced methods used by phishers in 2019.

In April, we reported on a campaign that carried out a new credential-phishing technique through the abuse of SingleFile, a web extension for Google Chrome and Mozilla Firefox. Cybercriminals used the otherwise non-malicious extension to produce identical copies of legitimate login pages that could steal victims' login credentials.

We also observed a credential-phishing technique capable of breaking two-factor authentication mechanisms by compromising one-time passwords (OTPs). This scheme, which was observed to have been prevalent in Japan in 2019, is directed toward online banking users. The phishing emails or SMS messages sent by the cybercriminals behind the scheme lead users to bogus online banking login pages.

If a user logs in to a phishing page, the user's credentials are stolen and simultaneously used by the cybercriminals to log in to the actual online banking login page of the spoofed bank. This then prompts the bank to verify the user's identity through an OTP. Once the user receives the OTP and enters it into the phishing page, the cybercriminals are able to steal it as well and use it to successfully compromise the user's account.

Cybercriminals had also managed to integrate the process of hijacking web search results for phishing. In 2019, they used poisoned Google search results to redirect phishing victims to an attacker-controlled page. To successfully do this, cybercriminals first funnel web traffic, which is hijacked from legitimate websites, to websites that they have control over. These websites then become the top Google search results for specific terms. The cybercriminals then send emails with links to the poisoned Google search results. Victims who click on the Google links and subsequently the top results are led to an attacker-controlled website before being redirected to a phishing website.

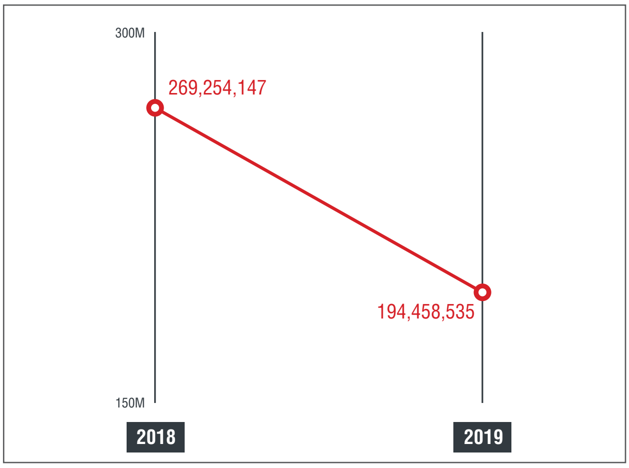


Figure 3: Detected attempts to visit phishing-related sites continued to decline: Year-on-year comparison of the number of instances of blocked access to non-unique phishing URLs (e.g., three instances of blocked access to the same URL counted as three). Source: Trend Micro Smart Protection Network infrastructure.

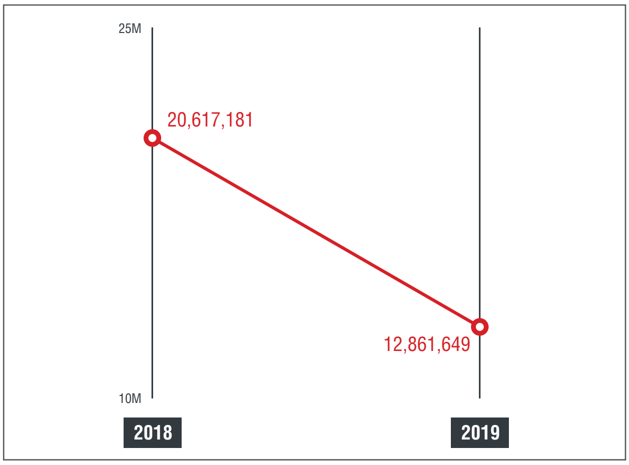


Figure 4: The number of users who would have been affected by phishing-related sites decreased: Year-on-year comparison of the number of instances of blocked access to phishing URLs by unique client IP address (e.g. one machine that attempted to access the same URL three times was counted as one). Source: Trend Micro Smart Protection Network infrastructure.

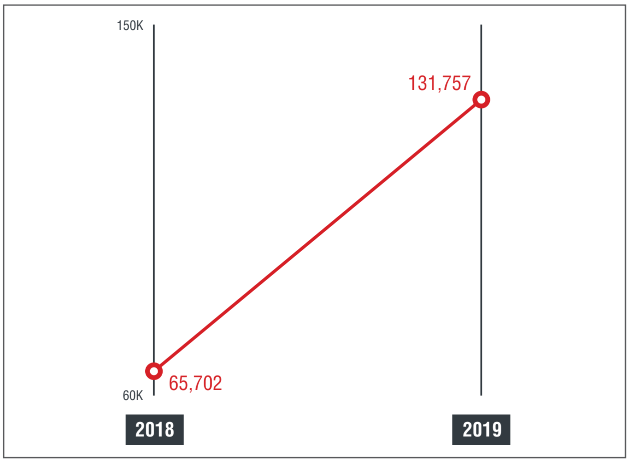


Figure 5: The number of blocked unique phishing URLs that spoofed Office 365 (including Outlook) doubled: Year-on-year comparison of the number of blocked unique Office 365-related phishing URLs. Source: Trend Micro Web Reputation Service.

Another notable technique seen in phishing campaigns in the past year was the use of custom '404 Not Found' pages. Instead of creating a single phishing website to redirect their victims to, cybercriminals register a domain and configure a custom '404 Not Found' page that poses as a login form to potential victims. Configuring a 404 error page allows cybercriminals to pair their domain with an infinite number of phishing landing pages.

BEC operators expand from traditional targets

Business email compromise (BEC) - which includes CEO fraud, bogus invoice, and account compromise, among other schemes - is a form of cybercrime that relies on social engineering to trick members of a target organisation into sending sensitive information and wiring funds to attackers. According to the FBI's Internet Crime Complaint Center (IC3), BEC had been the internet crime type with the biggest gains for cybercriminals. In 2019 alone, BEC operators bilked organisations of nearly USD 1.8 billion.

A trend we observed in 2019 showed BEC operators expanding from their traditional enterprise victims. Religious, educational, and nonprofit organisations were not spared from BEC attacks. And the public sector, particularly US government entities, became frequent targets.

In June, the city of Griffin, Georgia, lost over USD 800,000 to a BEC scam. BEC operators managed to trick city officials by posing as a longtime contractor and rerouting the stolen amounts in two separate transactions to a fraudulent bank account. One of the emails from the BEC operators requested a change in bank account information, which the recipient complied with. To make the scam appear more authentic, the scammers also used electronic invoices that contained information the city officials could verify.

A similar scheme was employed by BEC operators in October against the town of Erie, Colorado. They inveigled town officials into wiring more than USD 1 million to a fraudulent account by posing as a contractor that they were supposed to have been working with for a local bridge project.

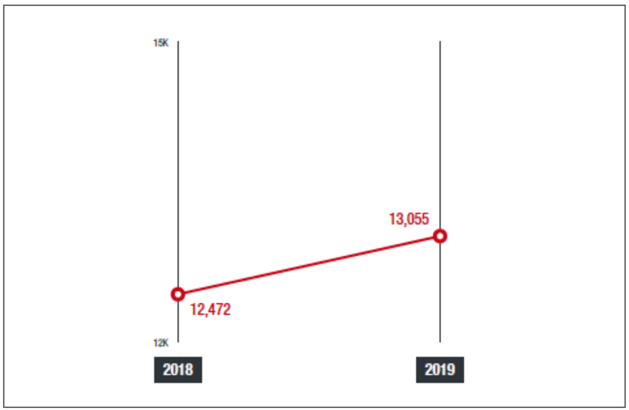


Figure 6: BEC attempts plateaued: Year-on-year comparison of the number of detections of BEC attempts. Note: Data refers to the number of BEC attempts seen, which does not indicate whether the attacks were successful. BEC attempts consist of CEO fraud. Source: Trend Micro Smart Protection Network infrastructure.

Our detections of BEC attempts, at around 13,000, registered only a 5% increase from the previous year. But this plateauing suggests that cybercriminals still recognised the high return on investment on BEC scams. Indeed, a

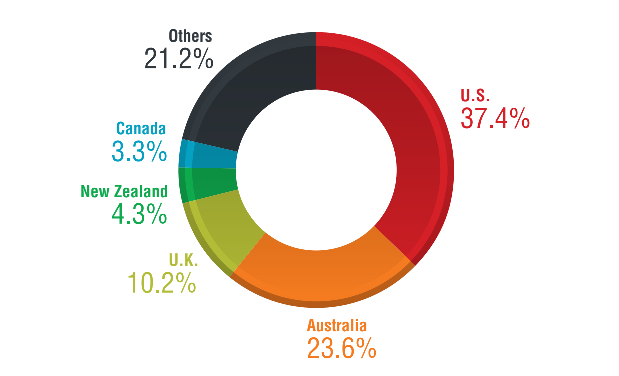


Figure 7: The majority of BEC attempts were detected in the US: Distribution of detections of BEC attempts by country. Note: Data refers to the number of BEC attempts seen, which does not indicate whether the attacks were successful. BEC attempts consist of CEO fraud. Source: Trend Micro Smart Protection Network infrastructure.

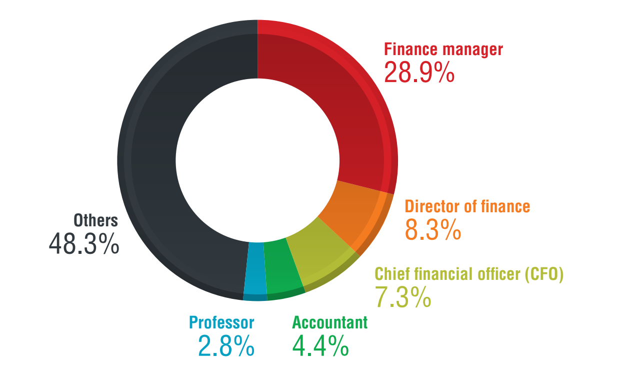


Figure 8: Positions other than high-ranking ones were among the top targeted positions in BEC attempts: Distribution of targeted positions in BEC attempts detected in 2019. Note: Data refers to a sample set of BEC attempts seen, which does not indicate whether the attacks were successful. BEC attempts consist of CEO fraud. Source: Trend Micro Smart Protection Network infrastructure.

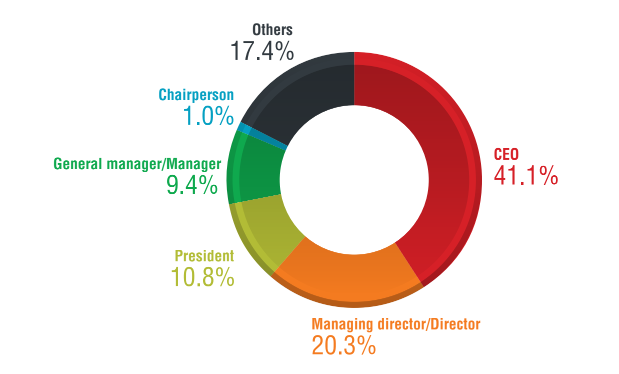


Figure 9: The CEO was still the most spoofed position in BEC attempts: Distribution of spoofed positions in BEC attempts detected in 2019. Note: Data refers to a sample set of BEC attempts seen, which does not indicate whether the attacks were successful. BEC attempts consist of CEO fraud. Source: Trend Micro Smart Protection Network infrastructure.

single successful attempt could make for a lucrative yield, even factoring in the research and other efforts that went behind it.

The BEC attempts that we detected came from different countries, with most of them detected in the US, Australia, and the UK. It should be noted that these countries are business hubs where headquarters of many multinational companies are based. Thus, while the number of attempts may be indicative of our customer user base distribution, it makes sense for a lot of these attempts to be directed towards them.

Among the top five most targeted positions in BEC attempts that we detected were professor and accountant, supporting our security prediction for 2019 that, apart from high-ranking company members, BEC scammers would target employees several levels down the company hierarchy. This appeared to be the case particularly in the education sector, where a number of BEC attacks were reported in the past year.

In our detections, positions of high operating authority were, unsurprisingly, still the most spoofed by scammers, with the CEO impersonated in the majority of BEC attempts.

Critical vulnerabilities threaten old and new systems alike

BlueKeep vulnerability amplifies risks faced by legacy systems

The complexity of current and emerging threats has created a reality where a single unpatched vulnerability can put an entire organisation at great risk. One need look no further than the damage caused by the WannaCry ransomware outbreak in 2017 due to unpatched systems - more than 230,000 computer systems infected in 150 countries and approximately USD 4 billion in financial losses. Organisations that use legacy systems are facing even more serious risks as computers that run on outdated operating systems are at peril of vulnerabilities that are no longer addressed by security fixes.

Threats to legacy systems, specifically those developed by Microsoft, were amplified anew in May when the company released a security guidance for BlueKeep (CVE-2019-0708), a vulnerability in its Remote Desktop Protocol (RDP). BlueKeep affects Windows 7, Windows 2003, Windows Server 2008 R2, Windows Server 2008, and Windows XP - legacy systems that a number of enterprises continue to use in their daily operations. If successfully exploited, the vulnerability can be used for remote code execution (RCE) attacks via the Remote Desktop Services component of Windows.

BlueKeep was heavily covered in the media because of its potential damage to many systems, with almost a million reportedly affected by it. It was also deemed notable for its 'wormability', akin to how the vulnerability was used by the EternalBlue exploit to infect systems with the WannaCry, Petya, and Bad Rabbit ransomware. But despite experts' assertion of the severity of BlueKeep, more than 800,000 vulnerable systems remained unpatched two months after its disclosure.

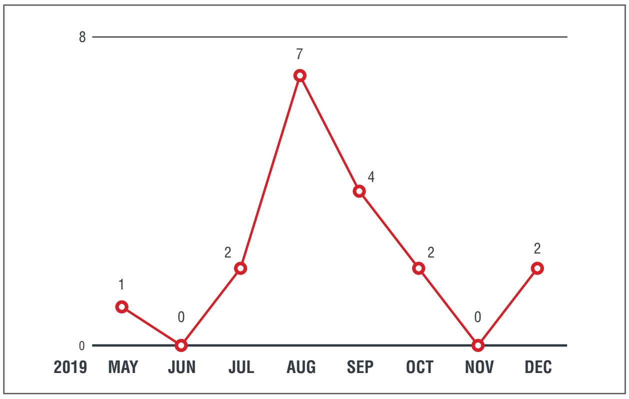


Figure 10: More vulnerabilities in RDP were disclosed in the wake of BlueKeep: The number of disclosed RDP-related vulnerabilities from May to December 2019. Source: Microsoft.

In September, threat actors started using BlueKeep in attacks to download and execute obfuscated PowerShell scripts, which installed and ensured the persistence of cryptocurrency miners. These attacks were a far cry from the scale of the outbreak caused by the aforementioned ransomware families, since missing in them was the self-propagating capability experts had warned about when BlueKeep first made headlines. In November, however, Microsoft stated that it could not discount the possibility that future attacks abusing the RDP flaw would be more damaging.

As early as 2018, the IC3, the FBI's centre for internet crime complaints, had warned administrators of RDP's susceptibility to exploits. In a public service announcement, it noted that malicious activity concerning RDP had been increasing since mid-late 2016, citing the sale of RDP access in the cybercriminal underground. Sure enough, threats that abuse RDP came into prominence when Microsoft issued its security guidance for BlueKeep in May 2019, and the disclosure of more RDP-related vulnerabilities ensued in the succeeding months.

RDP is often used by out-of-office workers and IT teams outsourced by organisations for remote computer access. The protocol provides convenience for 'anywhere working' collaboration and IT solution implementation, but it can also make for a convenient attack vector for threat actors. Attacks that effectively abuse RDP allow threat actors to take over affected computers, enabling them to access, process, and use files from drives. Worse, they can be a launching pad for further attacks that can take over the entire network. An open and accessible connection via RDP can allow cybercriminals to compromise devices and other resources connected to it.

Organisations are therefore advised not only to refrain from delaying patches for vulnerable systems but also to upgrade outdated systems such as Windows 7, which accounted for about a third of the operating system market in 2019 and support for which was ended by Microsoft in January 2020.

Disclosures of high-severity vulnerabilities more than double

In 2019, the Trend Micro Zero Day Initiative (ZDI) program published advisories covering 1,035 vulnerabilities, which were accumulated through collaboration efforts with independent researchers and vendors that released patches for the vulnerabilities ZDI reported to them.

The number of reported vulnerabilities decreased by almost a third from the previous year. However, it should be noted that the ones recorded in 2019 were greater in potential impact. Vulnerabilities that were rated with high severity, based on the Common Vulnerability Scoring System (CVSS), increased by 171% from the previous year and made up more than half of the total. Critical-severity bugs, on the other hand, decreased by 64% from 2018 and accounted for only 9% of the published advisories.

Disclosed ICS software-related bugs decline

In 2019, based on disclosures made via our ZDI program, the number of zero-day vulnerabilities and that of known or non-zero-day (n-day) vulnerabilities in software used in industrial control systems (ICSs) dropped by 79% and 11%, respectively, from the previous year.

Most of these flaws were found in human-machine interfaces (HMIs), which serve as hubs for managing critical infrastructures and monitoring different control systems that directly influence operations. As such, they can be abused by threat actors in attacks to cause disruptions.

Securing ICS environments is expected in the coming years to become an even more important imperative for enterprises that have them, as their adoption in the era of the industrial internet of things (IIoT) continues to widen. For one thing, the market for supervisory control and data acquisition (SCADA), a subset of ICSs, is forecast to grow to USD 15.2 billion by 2024.

Multiple botnet attacks exploit common IoT device flaws

The number of IoT devices is expected to grow to 22 billion by 2025. The prevalence of these devices in homes, offices, and cities has afforded people opportunities to take advantage of one of the most important technologies of the modern era. But as with any widely used technology, cybercriminals have also turned the IoT into a platform for conducting attacks.

Cybercriminals turn to IoT devices to take advantage of their often vulnerable state. Because patching them can be slow and problematic, IoT devices tend to be vulnerable for longer than traditional computing systems. This reality paved the way for the repeated use of old and known IoT device vulnerabilities by multiple botnets in 2019.

In April, for instance, we reported on a variant of the notorious Mirai malware (detected by Trend Micro as Trojan.Linux.MIRAI.SMMR1) that uses multiple exploits to target various routers and other IoT devices. A month later, we highlighted another Mirai variant (Backdoor.Linux.MIRAI.VWIPT), which exploits some of the flaws abused by the former, including an arbitrary command execution vulnerability (CVE-2017-17215) in Huawei HG532 routers.

This latter Mirai variant also notably exploited a remote arbitrary command execution vulnerability (CVE-2016-6277) in Netgear R6400 and R7000 routers. This vulnerability, in turn, is also part of the exploit arsenal of an Echobot botnet variant that uses more than 50 exploits and targets routers, network-attached storage devices, security cameras, smart home hubs, and other devices.

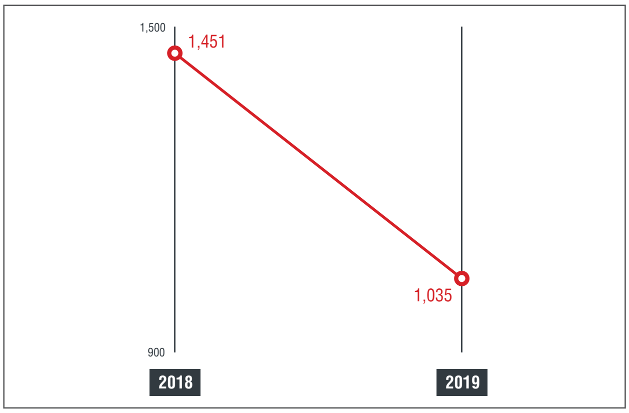


Figure 11: The number of published advisories decreased: Year-on-year comparison of the number of vulnerabilities disclosed via our ZDI program. Source: Trend Micro Zero Day Initiative program.

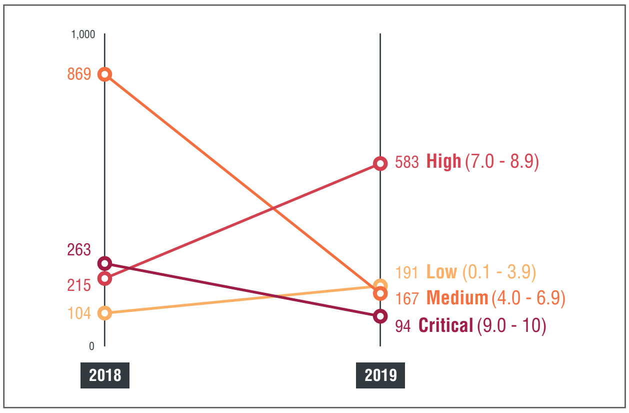


Figure 12: High-severity vulnerabilities increased more than twofold: Year-on-year comparison of the severity breakdown, based on the CVSS, of vulnerabilities disclosed via our ZDI program. Source: Trend Micro Zero Day Initiative program.

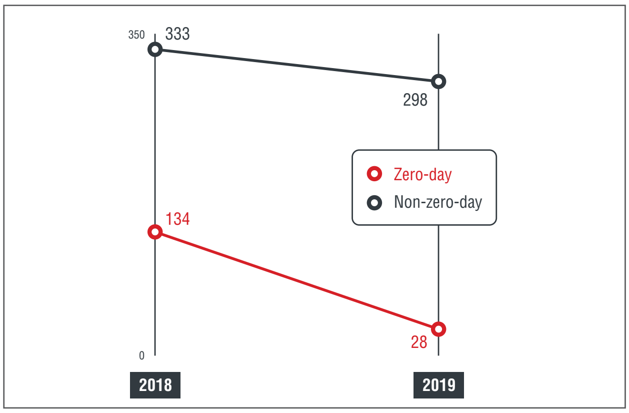


Figure 13: Disclosures of ICS software-related zero-day vulnerabilities decreased considerably: Year-on-year comparison of the number of ICS-related vulnerabilities disclosed via our ZDI program. Source: Trend Micro Zero Day Initiative program.

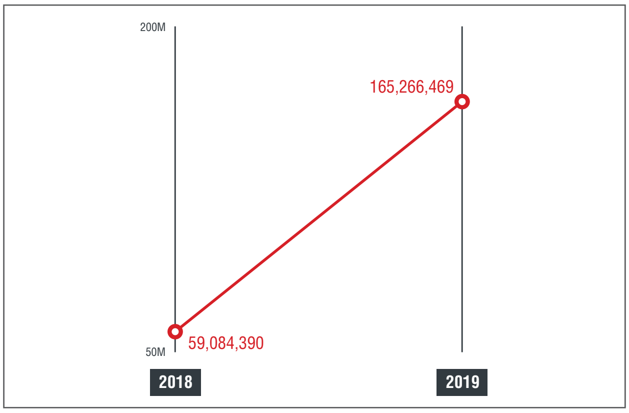


Figure 14: Brute-force logins surged: Year-on-year comparison of the number of triggered inbound and outbound events involving brute-force logins. Source: Trend Micro Smart Home Network solution.

Another pair of botnet variants that was found exploiting a common exploit was Neko and Momentum, which we reported in July and December, respectively, to have exploited a command execution vulnerability (CVE-2014-8361) in Realtek SDK-based routers.

Cybercriminals are also known to use brute-force attacks, in which they try out a large number of consecutive login credential guesses to gain access to unsecure devices. They typically use leaked, common, or even default usernames and passwords for their brute-force attempts, taking advantage of many IoT adopters' failure to change and update their devices' credentials. Based on our telemetry, which included feedback from third-party routers, the number of events involving brute-force logins in 2019 was nearly triple the corresponding count in 2018.

Threats seep through gaps in supply chains and development pipelines

Magecart supply chain attacks hit e-commerce websites

The past year saw a rise in cases of supply chain attacks, or attacks that compromise a service or organisation through an external partner or third-party provider that has access to its data or systems. And nowhere was this observation more evident than in the attacks tied to Magecart, a consortium of hacking groups that compromise e-commerce websites usually by going after their third-party shopping cart systems, such as Magento or OpenCart, to steal customer payment card information. As of October, Magecart had already compromised, either via supply chain attacks or directly, more than two million sites.

Among the Magecart campaigns we observed in 2019, two operations stood out. One of these was a campaign launched by Magecart Group 12. In January, we found that Magecart Group 12 had infected 277 e-commerce sites - including ticketing, touring, and flight booking sites, and online stores of apparel, cosmetic, and healthcare brands - by compromising their third-party advertising service. The group injected skimming code into the service's JavaScript library, enabling the group to steal the payment information entered by users on the sites.

The other notable card-skimming operation was one that we believe was launched by FIN6. From September to October, the campaign operated on 3,126 online shops hosted on one of the top e-commerce platforms in the market. The group injected malicious code into a JavaScript library provided by the e-commerce platform to their client shops, and this was followed by the loading of another JavaScript file stored on a cloud storage service. The loaded script was almost an exact replica of a normal JavaScript library but was subtly integrated with a credit card skimmer. Customers who visited the infected websites, most of whom were from the US, unknowingly submitted their credit card details to an exfiltration server.

The prevalence of supply chain attacks on e-commerce sites underlines the need for website owners to closely monitor security gaps in the platforms and services that they use and to implement stronger authentication mechanisms. For their part, users should keep an eye out for red flags when visiting e-commerce sites, especially since the number of reported cases of victims keeps on growing. In Japan, the pervasiveness of card skimming in e-commerce sites prompted the government to issue a warning to users in 2019.

Threats to software development tools and platforms rise

DevOps is a range of tools and cultural philosophies for streamlining software or application release cycles. This approach has been helpful for organisations that want improved quality, security, and scalability for software development. But while DevOps has given organisations an option for a faster and more efficient development process, the security aspect of it is sometimes overlooked, allowing threat actors to take advantage of components in the process with exploits and malicious code. For instance, there can be a tendency not to hold external parties to the same security standards implemented by the organisations themselves, which can lead to attacks such as code tampering, a technique often used in supply chain attacks. The process DevOps practitioners are operating in should take this and other security issues into account to avoid system compromise. Threat actors can undermine the development pipeline of an enterprise by interfering with a part of its software supply chain, and gaps in DevOps tools and platforms - such as those observed in 2019 - could enable them achieve that objective.

In June, we spotted an API misconfiguration in the open-source version of the popular DevOps tool Docker Engine - Community that could allow attackers to compromise containers and run AESDDoS, a Linux botnet malware variant. The execution of the malware enables attackers to take over the host and gain remote access to servers and hardware resources. Also in the same month, the developers of the widely used container orchestration system Kubernetes disclosed a high-severity vulnerability (CVE-2019-11246) in its command-line interface. Successfully exploiting the flaw could result in a directory traversal, enabling an attacker to use a malicious container to create or replace files in an affected workstation.

In July, we discovered security weaknesses in Jenkins, an automation server also used by practitioners, that could subject it to attacks. We observed that a user account with insufficient privileges could gain administrator rights over Jenkins, potentially allowing an attacker to perform RCE on its master machine. This risk stems from the improper configuration of the automation server's security settings. In August, we also reported about four vulnerabilities that affect Jenkins plugins whose successful exploitation could lead to the theft of sensitive user credentials.

Unsecure Docker hosts were also subjected to a variety of attacks in the past year, including one that involved cryptocurrency-mining malware, which was uncovered in October. Targeted hosts that lacked authentication measures were infected with the malware. This incident resulted in the infection of more than 2,000 Docker hosts by a worm that discreetly used them to mine Monero.

Poor software development practices can allow attackers to compromise DevOps tools and platforms, with the potential damage extending to organisations' physical, virtual, cloud, and container environments. As illustrated by two of the aforementioned examples, improper configuration of security settings could lead to system compromise. In addition, attackers could infect systems if the integrity of the source code, compiler libraries, and binaries, among others, are not properly maintained and cross-validated.

The research

The primary source of data is Trend Micro's Smart Protection Network (SPN), a global repository of threat intelligence. The data is collected from Trend Micro customers who have enabled the feedback mechanism from their products and solutions, allowing Trend Micro to collect threat data and provide better protection. All detected threats are subsequently removed from the customers' IT environment.

Disclaimer

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice.

(Part 2, the final part of the edited report, will be included in the August 2020 Issue of 'The Singapore Engineer')

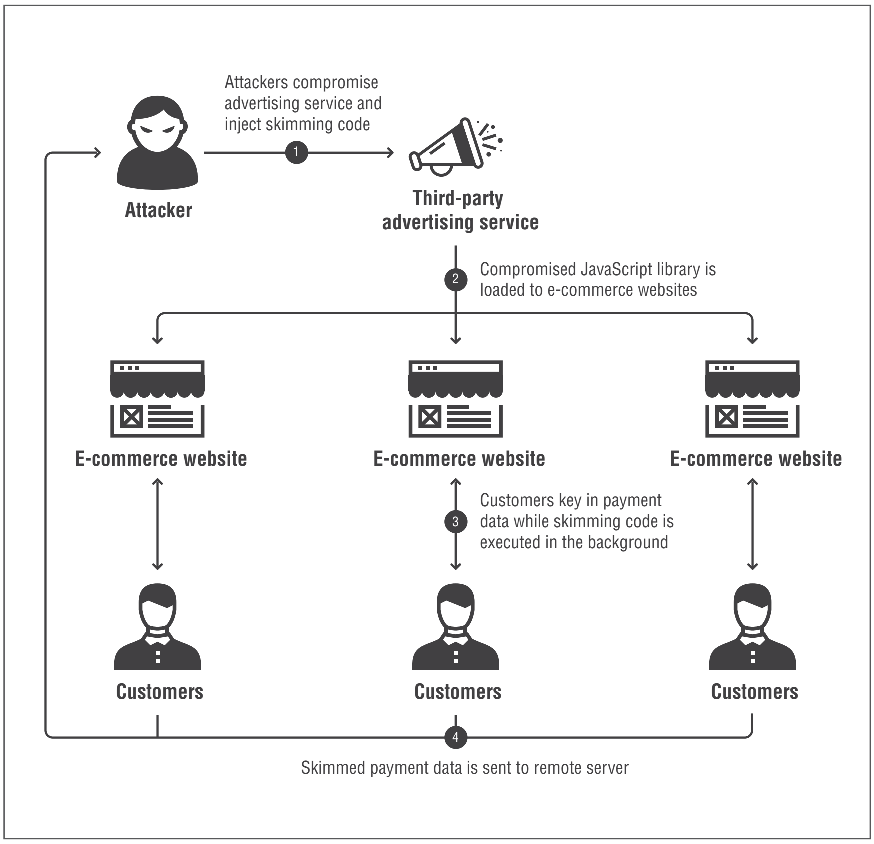

Attackers compromise advertising service and inject skimming code
1
Attacker
Third-party advertising service
2
Compromised JavaScript library is loaded to e-commerce websites
E-commerce website
E-commerce website
E-commerce website
3
Customers key in payment data while skimming code is executed in the background
Customers
Customers
Customers
4
Skimmed payment data is sent to remote server

Figure 15: Magecart Group 12 compromised e-commerce sites by breaching a third-party advertising service: The infection chain of Magecart Group 12's campaign.

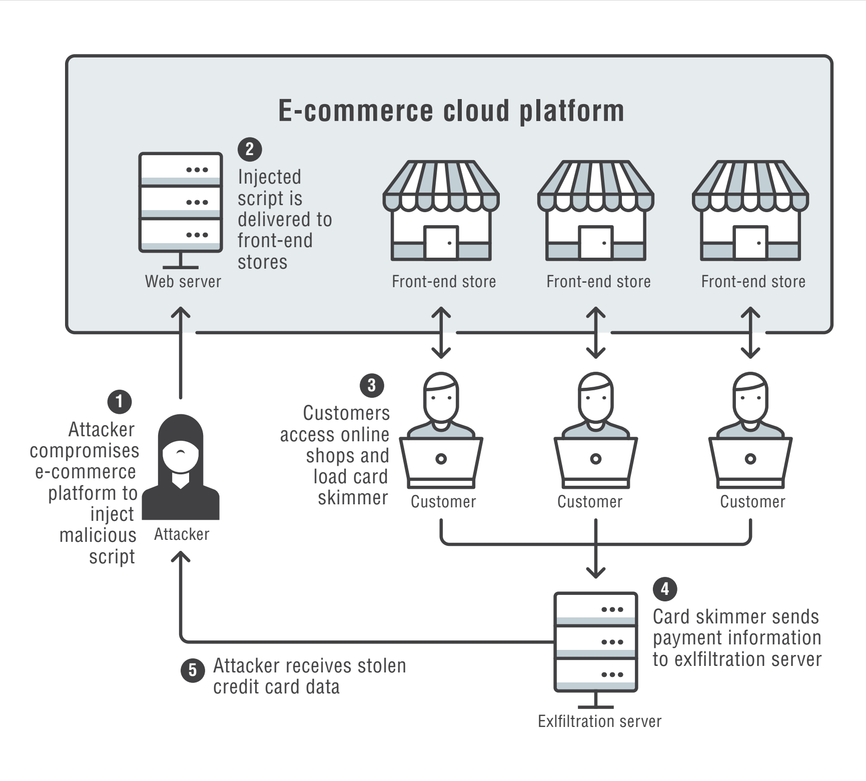

E-commerce cloud platform
2
Injected script is delivered to front-end stores
Web server
Front-end store
Front-end store
Front-end store
1
Attacker compromises e-commerce platform to inject malicious script
Attacker
3
Customers access online shops and load card skimmer
Customer
Customer
Customer
4
Card skimmer sends payment information to exlfiltration server
5
Attacker receives stolen credit card data
Exlfiltration server

Figure 16: FIN6 compromised sites hosted on one of the top e-commerce platforms in the market: The infection chain of FIN6's campaign.

SOLUSTAR UNVEILS WORLD'S FIRST SELF-CLEANSING DISINFECTING ROBOT

Solubots Pte Ltd, a subsidiary of Solustar Pte Ltd, a company that develops robots, recently unveiled the Solubots (Self-Cleansing) Disinfecting Robot, or SDR. Coupling patented self-cleansing technology with the autonomous or remote control function, this Made-in-Singapore innovation is said to eliminate the risk to personnel engaged in disinfecting work of exposure to COVID-19 infection.

The SDR's exclusive bell-shaped fibreglass casing with streamlined surfaces allows disinfectant droplets to cover target areas entirely, and fluids to drain away effectively, during any disinfecting process. In addition, the absence of protuberances, such as bolts and nuts on the SDR, commonly seen in similar robots, prevents foreign matter such as viruses from gathering and residing on its body.

Capable of shooting strong jets of disinfecting solution carrying chlorine or hydrogen peroxide, the robot is designed for killing coronaviruses. At about 8.5 microns in size, the disinfectant droplets are small enough to float in the air to increase treatment coverage.

The SDR can operate in two modes - remote controlled for affected areas and with autonomous navigation capability for general disinfecting. For affected areas, the operator can use a joystick, tablet or mobile phone to remotely control the spraying of disinfectant into nooks and crannies, with the aid of two water-resistant cameras. For general disinfecting, the robot can assume the autonomous navigation mode with built-in lidar and ultrasonic sensors to avoid obstacles such as glass.

The robot can be used in both inhabited and uninhabited spaces - an advantage over ultraviolet-C (UV-C) robots that require target spaces to be vacated due to health risks posed by UV-C light.

Measuring only 1.2 m in height and 0.7 m in width, the SDR's compact form can fit into small spaces, such as hospital rooms, with ease. Capable of treating a space with a volume of about 27 m^3 (or about 8.5 m^2 x 3 m) per minute, it can complete disinfecting a typical hospital room in about 15 to 30 minutes.

Maintenance for the SDR is made easy with built-in LED indicators for water level, battery power and error messages.

Currently in the trial stage, the SDR will be distributed by a fulfilment partner, NEC Asia Pte Ltd, both locally and in Southeast Asia.

"We are proud to partner Solustar in bringing this disinfecting robot to the market, not only in Singapore but also in the region and beyond. Many of our customers face the same challenge of a lack of manpower for disinfecting and sanitising their premises. The use of robotics will certainly go a long way in keeping people safe and places clean. We find this a very meaningful venture as we combine our resources and expertise to fight the virus", said Ms Vivian Tay, Senior Vice President, NEC Asia Pacific.

The SDR in action.

A close up of the spray nozzle on the SDR.

"We are excited about SDR as it offers distinctive solutions to overcome key challenges faced in carrying out disinfection operations, during the COVID-19 pandemic. Our immediate priority is to work with hospitals, the government, commercial offices, public space operators and other organisations to deploy the robot to make a difference in Singapore's fight against COVID-19. SDR can also be rolled out in trains, airports and hotel lobbies to safeguard the interests of our population", said Mr Louis Loo, Chief Executive Officer of Solustar.

A trailblazer in the robotics field, Solustar is also the manufacturer of the VAL concierge robot series.

Solubots is supported as an incubatee company by the IES-Incubator and Accelerator (IES-INCA), the technology incubation arm of the Institution of Engineers, Singapore (IES).

IES-INCA focuses on supporting technopreneurs in commercialising deep tech innovations to impact the industry and people's lives.

"The SDR automates the tedious work of disinfecting facilities and will be a key tool to help keep spaces virus-free. Robotics is one of the key focus areas of IES-INCA and we are excited to support local companies such as Solustar to develop innovative solutions that will address the needs of Singapore", said Mr Andy Wee, General Manager of IES-INCA.

Solustar Pte Ltd

Founded in 2013, Solustar Pte Ltd is a Singapore robotic and software development company focusing on developing enterprise grade applications for businesses and consumers. Solustar specialises in robotics, augmented reality (AR) and smart name cards. Its inventions include Solusight, an AR platform; Solucardz, a smart name card; and the VAL series of social humanoid robots.

Engineering team develops disinfection robot to battle viruses

In just one week, Siemens and Aucma, one of China's largest manufacturers of refrigeration equipment and other household appliances, have developed an idea into a prototype for an intelligent disinfection robot which will soon join the battle against Coronavirus and other viruses not only in hospitals but also in schools, offices, manufacturing sites and other public places, to support the resumption of work and production.

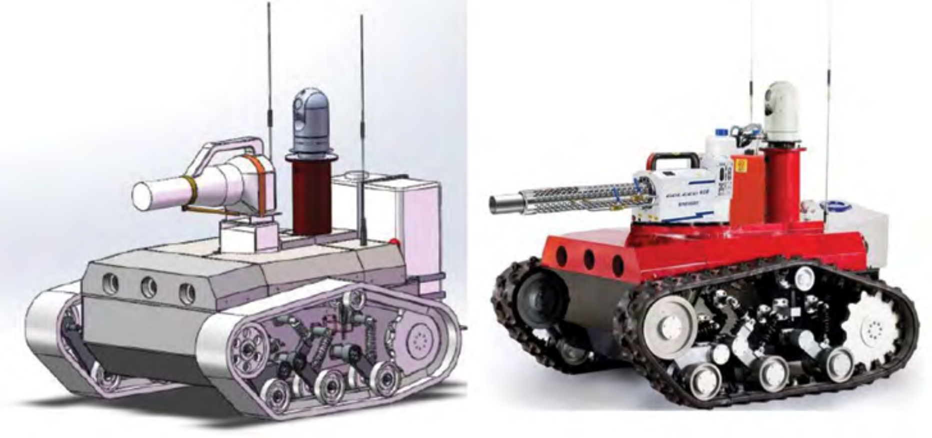
The electric robot can disinfect up to 36,000 m² in one hour and features a robust chassis that can overcome obstacles and navigate slopes.

Since the COVID-19 outbreak, there has been an urgent need in many hospitals for disinfection robots that can free people from having to disinfect high-risk areas.

Led by initiator Yu Qi, Head of Siemens China's Research Group for Advanced Manufacturing Automation in Qingdao, a team of 10 specialists with a broad mix of experience and expertise were confident that they could develop a new type of robot in a short period of time. The work is being carried out at the laboratory for robotic applications, co-established by Siemens and Aucma, where the focus is on developing special robots, unmanned vehicles, industrial robots, and intelligent equipment.

Most disinfection robots combine a petrol-driven mistoriser gun with an electric chassis. However, on-site refuelling of robots is neither clean nor convenient. The team therefore decided to develop purely electric disinfection robots to better cater to the needs of hospitals. The greatest challenges for the developers included ensuring maximum sterilisation impact with less disinfectant consumption and providing 360° coverage even in confined areas.

Powered by a lithium battery, a robot with double mistoriser guns can disinfect 20,000 m² to 36,000 m² in one hour. A 360° camera platform on the top transmits videos and information in real-time, coupled with an intelligent vision algorithm that allows the operator to remotely locate affected areas and prevent the spread of infectious diseases at low cost. To make the robots operate easily on various road surfaces, the team adopted a caterpillar chassis instead of wheels, to improve their ability to surmount obstacles and handle slopes.



In just one week, Siemens and Aucma developed an idea into a prototype for an intelligent disinfection robot. Each mistoriser gun can be rotated through 360°, enabling 100% sterilisation even in confined areas.

ROBOTMASTER

VERSION 7.2 RELEASED

Hypertherm, a US-based manufacturer of industrial cutting systems and software, has announced a new version update to Robotmaster V7, its CAD/CAM-based offline robot programming software. This new release contains targeted features and enhancements designed to generate greater efficiency and profitability for customers.

The update boasts several new features.

Path Transform

Path Transform allows users to copy, move, array, or mirror the paths in different or multiple locations on the part. This new feature eliminates redundant work and expedites the programming.

Intelligent cell and tooling creation

Integrators, partners, and end-users can now set up their robotic cell inside Robotmaster. Its intuitive user interface with real-time visual feedback enables users to calibrate, optimise, validate, and commission their robotic cell and tooling up to 10 times faster and with ease.

Welding tools

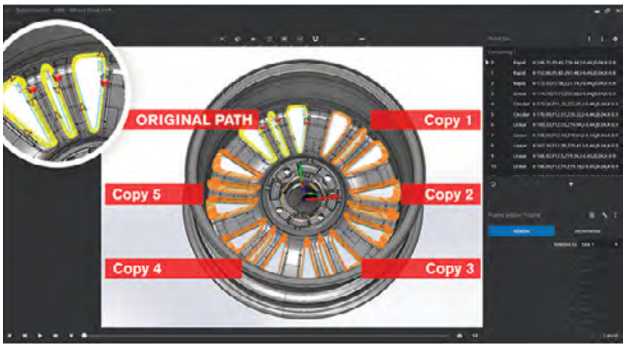
The new welding tools highlight how easy path creation in welding has become. The new welding selection method improves path creation in a visual way, which virtually eliminates the need to modify the geometry to select the welding seams while minimising the number of clicks. This method and the new touch-sensing grouping not only makes the process up to 10 times faster but also simplifies the overall workflow.

Geometry Filtering

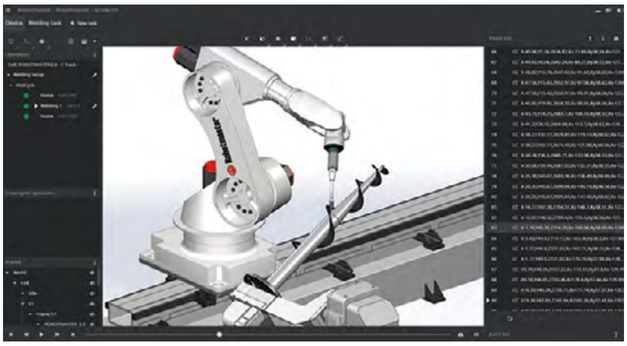
The new Geometry Filtering feature automatically filters out bad geometry edges to create quality paths, without worrying about bad geometry edges being unusable. The geometry filtering not only allows for cleaner path creation, but also facilitates smoother robotic motion.

Video tutorials

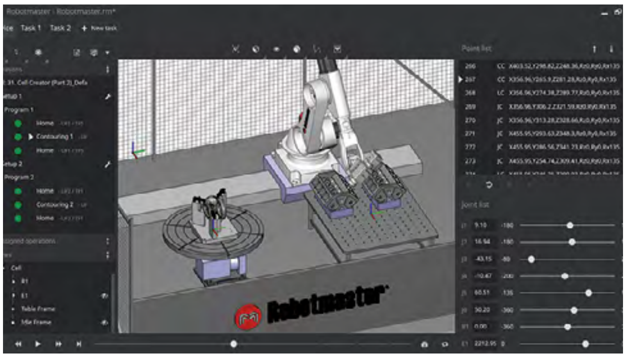
The full potential of the software can be maximised using the new library of video tutorials, which includes step-by-step part programming videos and the new Cell and Tool Editor tutorials.



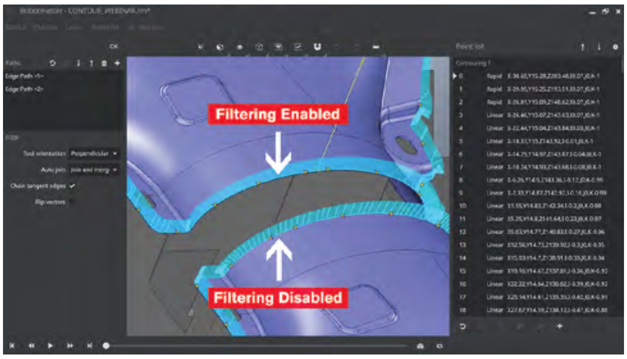
Path Transform allows users to copy, move, array, or mirror the paths in different or multiple locations on the part.



The new welding tools highlight how easy path creation in welding has become.



Integrators, partners, and end-users can now set up their robotic cell inside Robotmaster.



The new Geometry Filtering feature automatically filters out bad geometry edges to create quality paths.

NEW RUGGED LAPTOP NOW AVAILABLE

Getac Technology Corporation has recently unveiled its B360 fully rugged laptop, setting a new benchmark for innovation in the rugged computing industry. Fully engineered for 5G, the B360 boasts best-in-class computing speed, brightness, and rugged reliability, resulting in a highly advanced mobile solution that is suitable for challenging working conditions.

The B360 runs on the 10th Generation Intel Core Processor which, according to Getac, makes it the fastest fully rugged laptop on the market, capable of running large numbers of applications simultaneously without any impact on performance. A 1,400 nits Full HD display as standard - the brightest in Getac's computer line-up - is also said to be unrivalled in the fully rugged laptop class.

Getac builds all its devices rugged from the ground up. The B360 is no exception. The IP66 rating ensures it is completely protected from dust ingress, as well as high pressure water jets and spillages. The device can also withstand drops of up to 6 ft when in operation, while the latest MIL-STD 810H certification gives users complete confidence in its rugged reliability.

The B360 was developed based on Getac's extensive industry experience in creating comprehensive rugged computing solutions for specialised industry applications. As such, it is available in two distinct models at launch - the B360 which is ideally suited to the public safety, manufacturing, and utilities sectors, and the B360 Pro which is optimised for the defence sector.

In addition to best-in-class speed, brightness, and ruggedness, the B360 is the thinnest and lightest fully rugged laptop in its class. At just 34.9 mm thick and weighing 2.32 kg, it can be carried and operated for extensive periods of time without causing user fatigue. Despite such a compact form factor, the B360 boasts an expansive 13.3" LumiBond 2.0 display for maximum usability in all situations and weather conditions. The latest 802.11ax Wi-Fi delivers wireless speeds up to three times faster than previous generations. Dual hot-swappable batteries as standard ensure full-shift functionality between charges, while optional GPS makes mapping, surveying, and tracking in the field quick and easy.

The B360 Pro includes all the core technology specifications of the B360, along with a number of additional features and build options that are vital for military personnel. High-capacity, hot-swappable batteries deliver even more operating time between charges, while additional serial ports allow legacy and/or customised military equipment to be connected directly to the device. Customers also have the option to specify a PCMCIA, ExpressCard, or a discrete graphics card, as well as a DVD or Blu Ray drive as required.

The B360 is available now. The B360 Pro will be available in early July.

Getac Technology Corporation, a key subsidiary of MiTAC-Synnex Business Group from Taiwan, was established in 1989 as a joint-venture with GE Aerospace to supply defence electronic products. Today, Getac's business coverage includes rugged notebooks and tablet PCs not only for the military, but also for the automotive and process industry, the police, fire departments as well as utility, manufacturing, transportation and logistics customers. More information can be obtained from http://www.getac.com/apac.

Getac builds all its devices rugged from the ground up.

Getac's rugged notebooks and tablet PCs find application also in the automotive, process and manufacturing industries as well as in utilities, transportation and logistics sectors.

COVID-19 RELATED ASSISTANCE

FOR IES MEMBERS AND MEMBERS OF PROFESSIONAL REGISTRIES

The emergence of COVID-19 disrupted many engineers' jobs in Singapore, and caused a large number of engineering conferences, seminars and courses to be deferred or cancelled.

On 20 May 2020, the IES Council announced several initiatives to assist IES members and members of IES Professional Registries through this difficult period:

1. The annual subscription fee for IES membership was waived by 50 per cent for 2020/2021.
2. For Chartered Engineers, QECPs, SCEMs, EEO Assessors, and Civil & Structural Engineering RE/RTOs, a 100 per cent waiver of the CPD point requirements for their respective renewal periods was granted.
3. For ABC Waters Professionals and Mechanical & Electrical Engineering RE/RTOs, a 50 per cent waiver of the CPD point requirements for their respective renewal periods was granted.

Further details can be found on the IES website at http://bit.ly/IESwaiver. Any queries can be e-mailed to the IES Secretariat at ies@iesnet.org.sg.

We hope that the above adjustments would help alleviate members' burdens during this period, and wish for the continued good health and safety of all members.

NOTICE: IES 54TH ANNUAL GENERAL MEETING

Notice is hereby given that the IES 54th Annual General Meeting (AGM) will be held online at 1.00 pm on Saturday, 25 July 2020, via Globibo's AGM platform, which utilises the Zoom video conference platform.

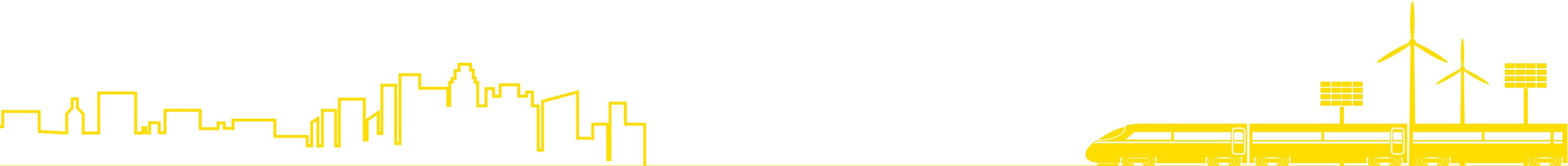
Registration will start at 11.00 am.

The minutes of the 53rd AGM (2019), President's Annual Report for Session 2019/20, Treasurer's Report, Statement of Accounts for Calendar Year 2019, annexes and proxy form have been posted at the Members' Corner on the IES website.

If you have not responded, please click on the RSVP button in the invitation email that was sent on 28 June. The deadline for response is 18 July 2020 (Saturday). You will receive a confirmation email with the e-AGM access link, your login details and instructions within 24 hours after registration.

Corporate Members who are unable to attend the e-AGM, but would like to vote for the resolutions are required to submit the completed Proxy Form (Annex C) via email or by post, to reach IES office latest by Thursday, 23 July 2020 (Please refer to Annex B for more information on the resolutions and voting instructions).

Associate Members are welcome to attend as Observers.



ADVERTISERS' INDEX

IES Chartered Engineer	Inside Front Cover	IES Railway Systems Handbook	Outside Back Cover
IES Membership	Inside Back Cover		

THE HEART & VOICE OF ENGINEERS

IES Membership

1) Professional Development

- Eligible for Chartered Engineers Certification Application (subject to registration criteria and conditions)
- Enjoy preferential rates for IES conferences, seminars and workshops
- Enjoy 10% to 15% discount for IES Academy Courses (T&Cs apply)

2) International Affiliations

- Interaction with overseas engineering institutions in joint programmes

3) Networking

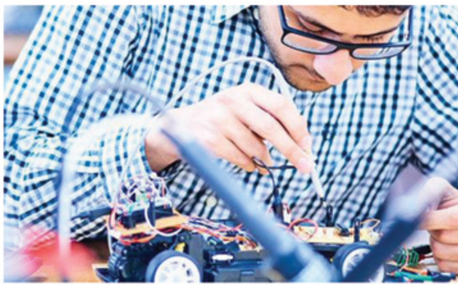
- Exclusive FREE Members' Night (T&Cs apply)
- Enjoy preferential rates for networking activities
- Join our Sports Interest Groups
- Join our Social Events

4) Communication

- Enjoy free subscription of IES weekly e-Newsletter
- Free monthly e-zine – The Singapore Engineer
- Free Annual IES Directory containing the business contacts of all members
- Get the latest updates on government regulations and the activities of allied institutions

5) Others

- Enjoy special rate for IES professional Indemnity Insurance Schemes
- Enjoy exclusive merchant benefits
- Free parking in IES premises
- Get a 5% discount off your membership subscription when you pay by GIRO (T&Cs apply)



Join Us!

www.ies.org.sg
64695000

RAILWAY SYSTEMS HANDBOOK

ON SALE NOW

S$35 / copy

(self collect; before GST)

Edited by:

Pang Hock Lye, John

Cheong Mun Kit, Eric

Published by: THE INSTITUTION OF ENGINEERS, SINGAPORE

Supported by: SINGAPORE RAIL ACADEMY

Scan here to order