YOKOGAWA

Co-innovating tomorrow™

OpreX™ Safety and Security

Cybersecurity Management

Risk Control Services for a Sustainable Value Maximization

Bulletin 43D07T31-02EN

1 McKinsey, “The Internet of Things”, 2015
2 Thomas Menze, in: Kapersky and ARC Advisory Group, “The state of industrial cybersecurtity”, July 2019

OpreX™ Safety and Security

OpreX™ stands for excellence in technology as well as solutions in industrial automation and control where co-innovating value for a prosperous future is consistently delivered to our business partners. This major brand consists of five categories: transformation, control, measurement, execution, and lifecycle.

The activities covered by OpreX™ Lifecycle contribute substantially to attain high levels of maintenance efficiency required for stable and efficient operation over the entire length of the plant lifecycle. They also strive to provide solutions that can further improve operability.

OpreX™ Safety and Security measures deliver comprehensive solutions that utilize the strategy of defense-in-depth with our safety & security lifecycle approach. Defense-in-depth is a multi-layered protection to enhance the cybersecurity protection level of the whole system. If one layer gets affected, other layers continue to protect against the attack.

In this way, we effectivley minimize both the safety and security risks for our customers’ systems.

1.2 – 3.7 TRILLION $

predicted value creation by using Manufacturing Analytics and Industrial Internet of Things in factories by 2025[1]

MORE THAN 80%

of the surveyed companies consider OT cyber defense measures to be very important. More than half are currently working to carry out their digital transformation, to comply with regulatory guidelines and to meet customer requirements.[2]

Facing the structural development of information and operational technology and the changing threat landscape, a reliable cybersecurity management is the key for gaining operational excellence. Moreover, it paves the way from industrial automation to industrial autonomy.

Choosing the right cybersecurity partner means choosing someone who not only observes progress, but actively works to shape the future.

This is how Yokogawa performs. And that is what makes our cybersecurity concepts the ideal to benefit from the power of digital transformation.

Operators are increasingly recognizing the most important security risks and are planning to implement comprehensive measures to ensure OT/ICS cybersecurity by solutions that rely not solely on technology.

Top initiatives for increasing OT/control system and network security

SANS State of OT/ICS Cybersecurity Survey 2019

37.3%

Perform security assessment or audit of control systems and control system network

29.5%

Invest in general cybersecurity awareness programs for IT, OT and hybrid IT/OT personnel

45.5%

Increase visibility of control system cyber assets and configurations

26.6%

Bridge IT and OT initiatives

28.3%

Implement anomaly and intrusion detection tools on control system networks

29.1%

Invest in cybersecurity education and training for IT, OT and hybrid IT/OT personnel

CAN YOU DO YOUR JOB WITHOUT RELIABLE SECURITY?

The process of digital transformation opens up immense opportunities. Comprehensive cybersecurity management is the basic precondition for exploiting them while reducing risk and enhancing organization resilience for long term stability.

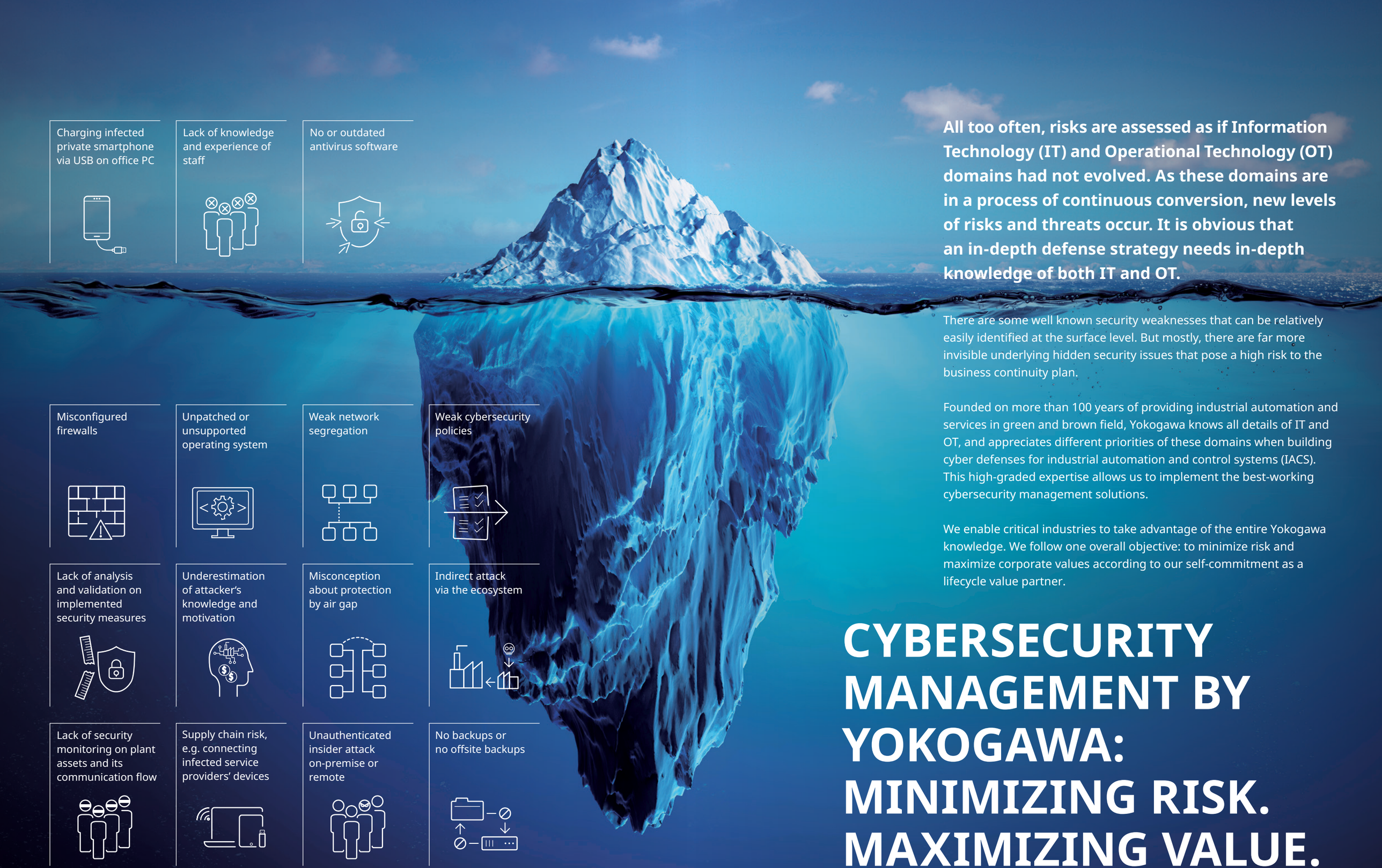
Modern industrial control systems are interwoven and interdependent. The need for a permanent data exchange between these delocalized or virtual systems will lead to a significant increase in data flow across more logical boundaries. Visibility is more on demand than ever.

The need for flexible production that can react quickly to customer requests is already evident today. Therefore, a cybersecurity management is required that not only protects but also opens up all potentialities of the Industrial Internet of Things.

Singular measures such as one-time antivirus software installations cannot meet the more demanding requirement of cybersecurity. This insight has reached almost all companies.

To provide high-end cybersecurity concepts, we at Yokogawa replaced solution-thinking with service-thinking. We actively support operators over the plant's entire life cycle, continually working on improvements in a close partnership with our customers.

That's what we understand by Co-innovating Tomorrow™.



All too often, risks are assessed as if Information Technology (IT) and Operational Technology (OT) domains had not evolved. As these domains are in a process of continuous conversion, new levels of risks and threats occur. It is obvious that an in-depth defense strategy needs in-depth knowledge of both IT and OT.

There are some well known security weaknesses that can be relatively easily identified at the surface level. But mostly, there are far more invisible underlying hidden security issues that pose a high risk to the business continuity plan.

Founded on more than 100 years of providing industrial automation and services in green and brown field, Yokogawa knows all details of IT and OT, and appreciates different priorities of these domains when building cyber defenses for industrial automation and control systems (IACS). This high-graded expertise allows us to implement the best-working cybersecurity management solutions.

We enable critical industries to take advantage of the entire Yokogawa knowledge. We follow one overall objective: to minimize risk and maximize corporate values according to our self-commitment as a lifecycle value partner.

CYBERSECURITY MANAGEMENT BY YOKOGAWA: MINIMIZING RISK. MAXIMIZING VALUE.

[1] Michael J. Assante and Robert M. Lee, in: SANS Institute, The Industrial Control System Cyber Kill Chain, October 2015
[2] SANS 2019 State of OT/ICS Cybersecurity Survey

JUST IN CASE: HOW MUCH TIME WILL THERE BE LEFT TO REACT PROPERLY?

The earlier a security compromise is detected and analyzed, the smaller the negative impact. It is strikingly simple: Data is as valuable as money. Availability and safety are of paramount priority, so improving cybersecurity is a matter of time.

Cybercrime is on the rise. The actors are constantly developing new technologies and methods to improve their activities. For months or years, long before an attack is executed, they collect information about plant equipment, OT and IT systems, employees and suppliers by using the ultimate hacking tools. As supply chains operate mostly just in time, disruptions will have cascading effects on plants and dependants. How much time do you think you have for response containment, eradication and recovery?

Yokogawa cybersecurity services enable you to act quickly and make the right decisions – not only in case of hacker attacks but in any other case of intentional or unintentional cybersecurity incident. We equip you with tools, people and processes that enable operation teams to detect and respond to irregularities at first view. We develop an exactly configured incident response plan and train its execution. And with our managed remote services, we are vigilant and ready to intervene – 24 hours a day, 7 days a week, 365 days a year.

< 36 MONTHS Intrusion to detection[1]

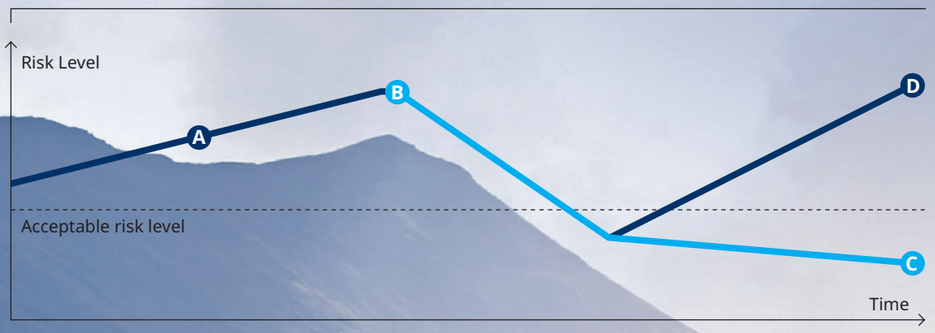
2–7 DAYS Compromise to detection[2]

6–24 HOURS Detection to containment[2]

2–7 DAYS Containment to remediation[2]

4–15 DAYS Downtime after security attack[2]

Security risk control concept



Risk level: the existing risk level that the industrial plant is facing
Acceptable risk level: the risk level that plant owners can accept as low as reasonably practical

A Security risk level rising
B Start of security roadmap and mitigation of risk by implementing countermeasures
C Maintaining countermeasures and applying improvement
D Without maintenance and improvement

Implementing cybersecurity management means ensuring the right balance between effort and reward. No matter what stage you are at: Yokogawa knows where and how to start the journey to a reliable cybersecurity.

It is common understanding that securing highly complex OT and IT systems with IT/OT integration is a considerable challenge. Which measures have priority, which can wait? How to implement cyber-security components smoothly and without interruption of production? Which human, temporal and financial resources are required?

With its long history in security, Yokogawa knows the answer to such questions. We are at home in all industries and countries, know best practices, standards and regulations, visions and innovations in OT and IT/OT integration – in a word, we know what to avoid and what to do.

With this expertise, Yokogawa creates a cybersecurity program which can be precisely tailored to your needs. We will guide you on your journey to the best working cyber risk management.

GAINING CYBER-SECURITY IS EASY: JUST START WITH THE FIRST STEP. AND DO NOT STOP.

LIFECYCLE CYBERSECURITY PROGRAM

Learn more about our cybersecurity services on www.yokogawa.com/cybersecurity

1 | AWARENESS & TRAINING

Effective cybersecurity risk management is not only about good technology and process. Human error due to a lack of cybersecurity knowledge and awareness leads to many cyber incidents nowadays. Educational awareness & trainings are essential cybersecurity controls that should be in place at the first step. Therefore, Yokogawa supports customers with tailored training programs, either remotely or on-site as needed, addressing appropriate contents to different functional levels, based on IEC 62443 while also considering required national and specific industrial standards.

2 | SECURITY RISK ASSESSMENT

Implementing an effective OT cybersecurity program requires intensive insights of the risks posed to the OT environment and understanding of the latest industrial standards and regulations. Yokogawa offers risk assessment from remote and at customers' sites to study the security risk within a plant's industrial network. This is followed up by gap analysis between existing plant and security requirements specified by IEC 62443. Delivered clear cut understanding of assessment results provides as a base to develop a comprehensive OT cybersecurity program effectively.

3 | POLICIES & PROCEDURES IMPROVEMENT

Complete and well defined policies and procedures are the most critical elements across organization in defining and executing a unified security strategy. With Yokogawa's best practice, off the shelf OT policy and procedure documents and comprehensive knowledge of IEC 62443, ISO/IEC 27001, NIST framework and national standards, Yokogawa's security consultants and experts support our customers in developing the most effective security policies & procedures. Hence, people and technology are connected more efficiently while avoiding any gaps.

4 | BUSINESS CASES DEVELOPMENT

The business case is a question of high importance: How much money should be invested in cybersecurity to achieve an acceptable risk level? Thus, Yokogawa collaborates closely with our customers. The budget is planned based on the outcome of the security risk assessment. Security risk levels are prioritized in conjunction with policies and procedures. Our consultants develop a realistic risk mitigation roadmap and implementation schedule together with customers to increase the plant's security level step by step by taking a lifecycle perspective.

5 | DESIGN & IMPLEMENTATION

In aligning complete risk assessment, company's policies, procedures and business cases, Yokogawa ensures deployment of the best hassle-free countermeasures. Our engineers and professionals are always trained to meet global security standards and qualifications. Standard security countermeasures, among others, are automated/manual security updates, user and access control design, firewall, unidirectional gateway, network segmentation design, secure remote access and backup & recovery.

6 | MANAGED OPERATION & MAINTENANCE

24/7 secured monitoring, analysis of network activities and overviewing security performance and compliance matrix not only reduce the critical cybersecurity burden on plant engineers but also provide effective protection against known and unknown cyber threats. Yokogawa's managed operation and maintenance services are designed securely to meet the customer's unique requirements and to ensure that implemented cybersecurity solutions are not deteriorating. Standard managed services, among others, are fully integrated and continuous security monitoring & maintenance, asset inventory management, threat analysis and incident response.

ONE OF THE STRONGEST REASONS FOR CHOOSING A PARTNER: TRUST

Experience and expertise are essential qualifications for a cybersecurity partner. We at Yokogawa believe that, besides safety, some of the key requirements of industrial production are indispensable, too: availability, efficiency and reliability.

Confidentiality and trustworthiness
We acknowledge that your trade secrets are your capital as much valuable as your data is. That is why we commit ourselves to secrecy. Protecting our services is as self-evident for a security provider: with the very highest security level. That is part of what established Yokogawa's world wide status as a trustworthy partner.

Lifecycle value approach
No matter which industry: Yokogawa paves the way to stable, safe operations. By focusing on long-term services for the entire plant's life cycle, we achieve maximum benefits for the operator.

We are exactly where we are needed
Depending on the particular needs and requirements, we work directly at customers' sites or headquarters or in our Security Operations Centers and/or Response Centers with the best security standards, as it is a matter of principle.

More than 100 years of history and outstanding knowledge
While leveraging core OT business and domain IT knowledge for more than 100 years, we are operating our specialized Security Laboratory to investigate leading edge technology and established a global network with offices around the world – a comprehensive knowledge pool which our experts can access at any time. That is what gives us our edge: We never start from zero.

Contributing to a better world: an obligation for us
We live in a world with limited resources. Making the best possible use of them and dealing responsibly with health and the environment is firmly anchored in Yokogawa's corporate philosophy. We support the Sustainable Development Goals as a company that seeks to build a safe and sustainable society by using its core measurement, control, and information technologies, while pursuing digital technology innovation and co-innovation with its customers to revolutionize productivity in a wide range of business processes.

Industrial cybersecurity certification and high level expertise
It is evident that Yokogawa's global security team are familiar with various security frameworks and they closely follow international standards and national guidelines.

SUSTAINABLE DEVELOPMENT GOALS

- ✓ NIST CSF
- ✓ GICSP
- ✓ NERC-CIP
- ✓ ISO/IEC 27000 SERIES
- ✓ IEC 62443 SERIES

www.yokogawa.com/cybersecurity

Design: www.illigenwolf.de

OpreX™ Through the comprehensive OpreX portfolio of products, services, and solutions, Yokogawa enables operational excellence across the enterprise.

Yokogawa Electric Corporation
World Headquarters
9-32, Nakacho 2-chome, Musashino-shi,
Tokyo 180-8750, Japan
https://www.yokogawa.com/

Yokogawa Corporation of America
12530 West Airport Blvd, Sugar Land, Texas
77478, USA
https://www.yokogawa.com/us/

Yokogawa América do Sul Ltda.
Alameda Xingu 850 Barueri CEP 06455-030
Barueri – SP, Brasil
https://www.yokogawa.com.br

Yokogawa Europe B. V.
Euroweg 2, 3825 HD Amersfoort,
The Netherlands
https://www.yokogawa.com/eu/

Yokogawa Electric CIS Ltd.
1, Samarskaya street, business center Novion,
Moscow, Russia, 129110
https://www.yokogawa.ru

Yokogawa China Co., Ltd.
Room 1801, Tower B, THE PLACE, No.100 Zunyi
Road, Changning District, Shanghai, China
https://www.yokogawa.com/cn/

Yokogawa Electric Korea Co., Ltd.
(Yokogawa B/D, Yangpyeong-dong 4-Ga),
21, Seonyu-ro 45-gil, Yeongdeungpo-gu,
Seoul, 07209, Korea
https://www.yokogawa.com/kr/

Yokogawa Engineering Asia Pte. Ltd.
5 Bedok South Road, Singapore 469270, Singapore
https://www.yokogawa.com/sg/

Yokogawa India Ltd.
Plot No.96, Electronic City Complex, Hosur Road,
Bangalore - 560 100, India
https://www.yokogawa.com/in/

Yokogawa Middle East & Africa B. S. C. (c)
P.O. Box 10070, Unit A7, Building 1320, Road 1516,
Block 115, BIIP, Al-Hidd, Kingdom of Bahrain
https://www.yokogawa.com/bh/

Represented by:

Printed in Japan, 311(KP) [Ed : 03/b]

Trademarks
All Brand product names of Yokogawa Electric Corporation in this Bulletin are either trademarks or registered trademarks of Yokogawa Electric Corporation.
All other company brand or product names in this bulletin are trademarks or registered trademarks of their respective holders.

Subject to change without notice.
All Rights Reserved. Copyright © 2020, Yokogawa Electric Corporation

YOKOGAWA Co-innovating tomorrow™