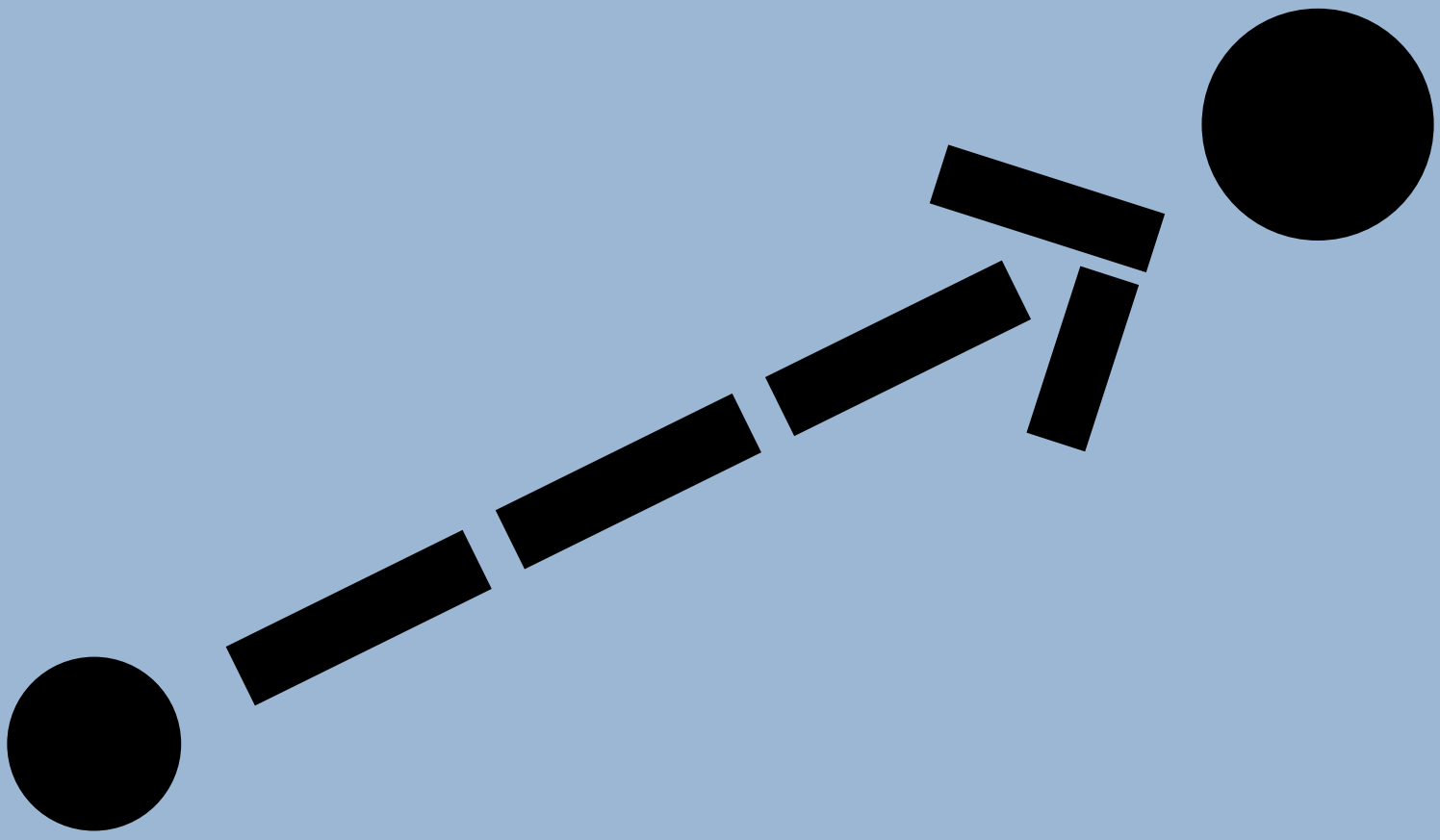
WHITEPAPER

The Complete Guide to Remote Access

From traditional industrial connections to Secure Remote Access purpose-built for OT



SECOMEA

About Secomea

Founded in 2008, Secomea has been catering to the OT remote access needs of manufacturers and machine builders for over 15 years.

Secomea is a Secure Remote Access (SRA) solution purpose-built for industrial networks and OT equipment. Over 9,500 customers around the world use it every day across thousands of sites to manage remote access to their machines, reduce cybersecurity risks, and prevent downtime.

Table of Contents

01

Reassessing old-fashioned access methods for enhanced OT security

There is no need to build the business case for industrial remote access today. Any modern manufacturing organization that wants to stay relevant and competitive acknowledges the cruciality of remote access and the countless benefits stemming from it.

Still, companies are seeking solutions and strategies to make their critical remote access operations more secure.

Preventing threats to OT is the main priority across the board, followed by improving cybersecurity, ensuring regulatory compliance, and lowering costs while enhancing user experience.

The traditional tools currently used fall short of being an effective strategy for OT remote access due to three main factors:

- **Manufacturers lack control over third-party access:** With multiple machine suppliers and as many remote access tools operating on the factory floor, third parties often have extensive access, sometimes even admin-level. Machine vendors can connect whenever they want, and there's no audit log for the asset owner to know what resources are being accessed, when, and what is being done. It's crucial for security strategies to focus on secure access management, precise control of access levels, and continuous monitoring of third-party activities. Unsurprisingly, handling vendors' access is the top reason why manufacturers look for OT remote access solutions.

- **The IT-OT convergence opens the door to cyber threats:** Admittedly, for a long time, cybersecurity was only a focal point in the IT domain. OT environments rarely needed dedicated protection against cyber-attacks because they were primarily local systems without network access. But that all changed with IT-OT convergence. OT appliances can use external networks for remote communication, maintenance, and upgrades, but this also exposes them to external threats on those networks. That's why ensuring IT security is not enough. More than ever, there's a need for dedicated OT security.

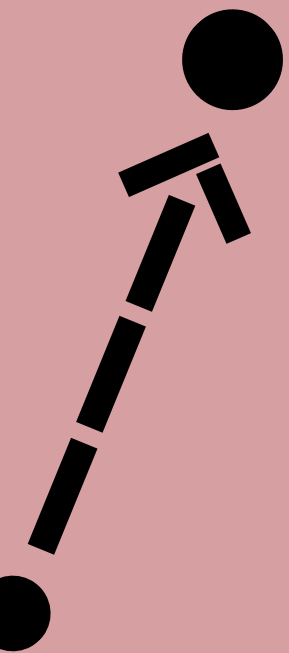
- **Tools designed for IT just won't cut it anymore:** Manufacturing organizations have been relying on IT-designed tools for remote access to operational technology (OT) systems. However, these tools have proven inadequate and leave security gaps that attackers can exploit. Traditional IT-centric solutions like VPNs, firewalls, Jump Servers, and Privileged Access Management (PAM) present outstanding challenges when used for OT, such as lack of visibility, inadequate user training, poor access control, and insufficient policy enforcement. Moreover, they face scalability challenges and cannot accommodate all OT use cases.

Overall, there is a pressing need for secure, scalable, and OT-specific remote access solutions that address the unique requirements and challenges of operational technology environments.

Manufacturing organizations need **tools designed to cater to OT priorities and handle OT complexities**.

And that's where Secure Remote Access **(SRA)** solutions **purpose-built** for OT systems and networks come into play.

This whitepaper looks at the roots of these manufacturing challenges and the inadequacy of existing tools juxtaposed with the benefits companies can gain by implementing a purpose-built OT remote access solution.



02

The challenge of third-party access in OT

OT environments rely heavily on third-party services for patching, troubleshooting, monitoring, inspection, maintenance demands, and risk mitigation.

According to Ponemon Institute research, three in four organizations allow third-party access to their OT environments. On average, 77 third parties are granted access to each of these companies. The main security challenges associated with third-party access are preventing unauthorized access (44%), aligning security priorities between IT and OT (43%), and controlling the extent of privileged access given to users (35%).

The more people and systems connect to your OT resources, the greater the risks

Historically, OT and industrial control systems (ICS) were completely isolated from the Internet and other networks, with only a specialized group of technicians skilled in managing and maintaining these systems. With a limited number of experts handling them, these systems faced reduced risks of damage. However, the current landscape has drastically changed.

Industrial infrastructure innovations such as cloud computing, OT/IT convergence, or even the rising remote work are advancing productivity and performance on one hand while creating new OT risks and vulnerabilities on the other.

These developments have somewhat blindsided the OT community. Security teams often lack awareness of how many internal and external users access their systems, not to mention the potential hidden entry points. Additionally, the absence of adequate session monitoring mechanisms opens further opportunities for attackers to target these critical systems, exacerbating the challenge of protecting them.

Third parties often request or receive overly generous access

Machine vendors often receive broad entry to the network, and they are sometimes even granted admin-level privileges. While that is usually based on an assumption of trustworthiness, even well-meaning contractors may lack the same security commitment as your employees and inadvertently facilitate major security breaches – which would cause significant financial and reputational damage to your organization, even if the third party is at fault.

Asset owners' security teams struggle to monitor and control these vendors' actions and their adherence to security protocols, resulting in a primarily reactive approach when breaches occur.

After all, you can't easily compel third-party vendors to install the company's proprietary security tools on their own devices. Yet, it is also unrealistic, expensive, and time-consuming to provide every vendor with a company-managed device. And that's all the more true considering that each of your third-party vendors has its own third parties - who have their own third parties - all linked in an ecosystem that you have no control over.

Given the potential harm they could inflict—whether by intention or accident—it is essential to treat all partners, vendors, suppliers, and contractors accessing corporate systems and resources as potential sources of risk. Traditional perimeter-based security models are insufficient; secure access management must become the core focus of cybersecurity strategies.

Security measures must enable the monitoring of their activities, precise adjustment of their access levels, and verification of their identities, all without hindering their effectiveness.

That is why, across all industries, managing and securing third-party access is the main motivation for adopting an OT remote access solution - as confirmed by Takepoint's Research Survey Report 2023.

03

IT-OT Convergence and emerging OT cyber threats

Until only five years ago, OT cyber threats were primarily a theoretical problem. Only 25% of attacks directly impacted OT networks and systems.

Since 2020, though, they have been increasing exponentially. OT cyberattacks are nearly doubling yearly, causing shutdowns and financial losses in hundreds of industrial sites globally.

Tactics and motivations evolved in 2023, when 68 attacks impacted over 500 OT sites, according to Waterfall's 2024 Threat Report. One in three companies reported that both OT and IT systems were affected by a cyberattack.

Hackers now target critical infrastructures, causing severe supply chain disruptions and logistical outages. Fortinet's 2023 State of Operational Technology and Cybersecurity Report states that over half of cyberattacks impacted discrete or process manufacturers in sub-industries such as electronics, automotive, marine, cosmetics, and metals. One of these attacks was cited as causing bankruptcy and mass layoffs, adding to two similar incidents in 2022.

2023 OT cyber-risks in numbers

While malware (56%) and phishing (49%) were the most common incidents reported in 2022, ransomware was responsible for 80% of successful attacks in 2023.

Phishing accounts for 85% of cyber threats to manufacturing businesses, and small businesses receive the highest rate of malicious emails.

Nearly 80% of organizations reported having over 100 IP-enabled OT devices in their OT environment.

Most of these companies stated that the average age of ICS systems across their organization is between 6 and 10 years old.

48% of larger companies have over 50 remote users connecting to their industrial environment daily.

Although cyber-attacks on large corporations often receive the most media attention, small businesses should not consider themselves out of the woods. Nearly half (46%) of data breaches happen in companies with less than 1,000 employees. On average, a cybersecurity event can cost a small business about $200,000.

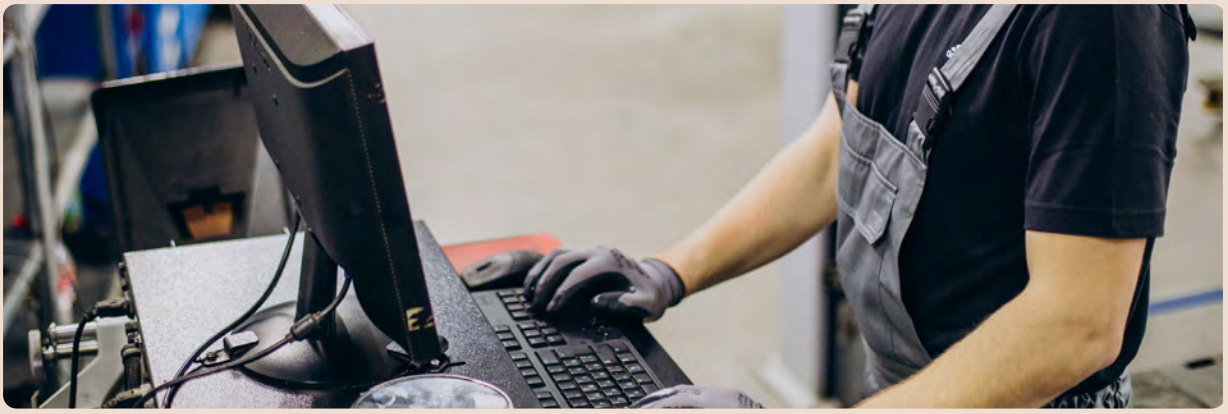
The number of connections grows proportionally with the company size, as does the attack surface. However, a bigger organization is likely to have a bigger budget and more expert staff to protect itself. On the other hand, a smaller company doesn't mean lower risks, as it may not have the resources required to secure its systems sufficiently.

Securing remote access is not a challenge exclusive to big organizations. Companies of all sizes express worries about the risks linked to remote access and generally hold little trust in the security measures currently in place.

Another critical problem faced in the industry is the growing cybersecurity talent shortage. Fortinet's 2023 Cybersecurity Skills Gap Global Research Report revealed that organizations are struggling to find skilled professionals to fill crucial security positions.

The results also show that OT cybersecurity experts are no longer coming from operations staff but from IT security leadership, so the influence on cybersecurity decisions is moving from OT production management to Information Technology professionals. 95% of organizations intend to place the responsibility for OT cybersecurity under a CISO within the coming year.

IT teams are pressured to become more knowledgeable about OT, and organizations are seeking and adopting security solutions encompassing their entire IT/OT infrastructure to lower their overall risk exposure.



04

The shortcomings of IT-centric tools when used for OT

Due to a lack of secure remote access solutions built specifically for OT, manufacturing organizations have been relying on IT-designed tools. These are far from ideal because they overlook factors that attain the specific nature of operational technology - i.e., its non-negotiable requirements.

The main challenges of the IT-OT convergence

OT systems typically fulfill mission-critical demands by operating continuously, 24/7, 365 days a year. IT-centric tools commonly require regular patching, which implies the interruption of OT processes, leading to costly downtime. The challenge lies in addressing security vulnerabilities while minimizing downtime, as critical functions cannot afford service interruptions for updates.

Not to mention that while most IT can, by design, be discovered and configured remotely, OT systems often don't offer similar visibility by default – as they were not originally designed for remote accessibility and standardized communication.

Moreover, the distributed nature of OT environments translates into a larger attack surface. Thereby, the need for administrators to see and manage all OT devices needs to be met – which can't easily be done without hardware gateway components connected to OT appliances (or software embedded, if applicable).

The technologies in place to protect IT/OT operations are proving inadequate

Despite their common deployment, most remote access tools in OT/ICS environments are IT-centric solutions that fail to meet the complex needs of OT systems.

The methods currently used, like VPNs and firewalls, are usually outdated, overly complicated, rigid, and susceptible to errors. They struggle to scale and cannot cover the full range of OT use cases, nor can they handle the requirements of widespread yet interconnected operations – not to mention that they are also often the primary avenues for attacks.

- **Traditional VPNs** are widespread thanks to their simplicity of implementation, which requires minimal changes to the existing infrastructure. Once connected via a VPN, remote users are placed on the same network as all operational assets, often lacking robust security measures. This setup generally grants either full or no access, with no room for granular or temporary access to specific assets.

  If a remote user's credentials are compromised or stolen, an attacker can easily access vulnerable OT assets. Additionally, even legitimate users could significantly jeopardize operational networks if they connect from devices infected with malware, which then spreads across the network connection—as VPNs don't offer malware scanning features.

- **IT-focused Zero Trust Network Access (ZTNA)** solutions offer an advancement over traditional VPNs for accessing IT networks. Yet, they fail to uphold layered security defenses within OT environments. Typically, ZTNA solutions need endpoint agents, which are unfeasible to implement on OT assets.

- **Firewalls** and **Access Control Lists (ACLs)** usually route remote OT traffic through a DMZ network. However, this often involves setting up hundreds or thousands of intricate firewall rules, which are laborious and complex to manage – which, in turn, creates operational difficulties and escalates the risk of ransomware, spoofing, and other cyberattacks and security breaches.

- **Jump Servers** are frequently used as an alternative to giving direct internet access to OT assets. Each remote user, however, must have an account on these servers, and these accounts soon multiply - often becoming inactive yet seldom removed, creating ideal opportunities for cyber attackers. This vulnerability compels operators to invest in expensive **Privileged Access Management (PAM) tools**, adding to the accumulation of underutilized tools without enhancing security. Thus, jump servers and PAM solutions fall short of being an effective strategy for OT remote access.

Companies rely on these remote access workarounds out of operational necessity, yet they acknowledge that they are not adequate long-term solutions.

Lack of visibility (55%), inadequate user education and training (54%), and weak access control (53%) are cited as the top three concerns, followed by outdated operating systems (52%), insufficient policy enforcement (47%), and fear of unauthorized access (44%).

Threats to operational safety (75%), Advanced Persistent Threats (67%), and misconfigurations or errors (59%) are identified as the primary risks associated with remote access to industrial environments.

05

The need for OT-specific Secure Remote Access (SRA)

As industrial infrastructure evolves, there is a growing demand for a flexible and robust remote access solution specifically designed for OT and ICS environments.

Manufacturing organizations require tools that are designed specifically to meet the unique demands and intricacies of operational technology (OT). This is where specialized Secure Remote Access (SRA) solutions, tailored for OT systems and networks, become essential.

Typical use cases

Drivers and benefits

By supporting **remote work** and secure access to corporate resources from anywhere with an internet connection, SRA solutions enable **flexibility**—which is especially valuable during emergencies or in a global workforce. What's more, organizations can tap into a **global talent pool** by hiring remote workers from various geographic locations, accessing specialized skills, and reducing the impact of talent shortages.

SRA solutions play a crucial role in **business continuity** plans. They reduce the impact of crises by ensuring that operations can continue even when employees cannot physically be present due to emergencies or unexpected events like **natural disasters**, **pandemics**, **and global crises**. Safe operations can be maintained continuously at remote, hard-to-reach sites, even in potentially dangerous places and times.

SRA tools lead to **lower expenses and higher cost-efficiency**, as there is no need to wait and pay for a technician to visit the location of the device in need of assistance. Data analytics paves the way for predictive maintenance – which, in turn, leads to reduced operational and support costs. Higher visibility on production environments and auditing capabilities enable **data-driven decisions** based on OT-IT converged data.

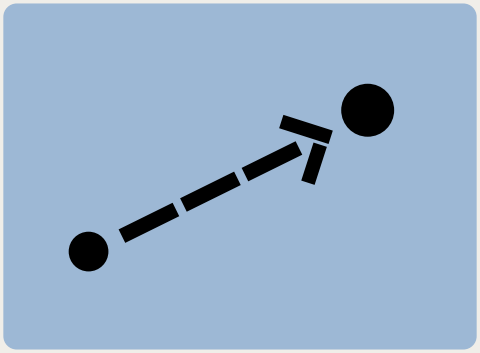
Real-time monitoring lets you recognize patterns and anomalies to **avoid unplanned downtime**. Engineers can rapidly troubleshoot machines and recover from production issues. Ultimately, secure remote access solutions **improve asset management**, **process automation**, **and performance efficiency** from equipment handling to resource utilization, from maintenance scheduling to regulatory compliance and safety measures.

06

Secomea's solution: Secure Remote Access purpose-built for OT

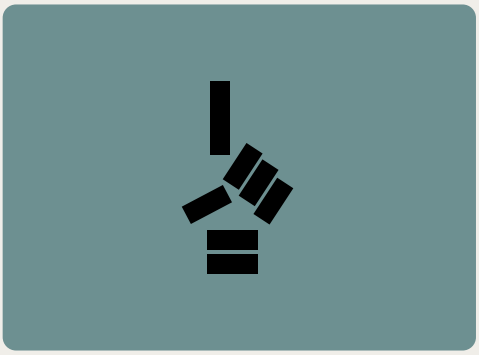
Secomea is a Secure Remote Access (SRA) solution purpose-built for industrial networks and OT equipment. It includes all the software and hardware components needed for performing remote access and maintenance tasks—from remote programming and troubleshooting to data-driven decision-making.

As a turnkey solution, Secomea can be implemented at record speed, and it's ready to use with ease, even by non-IT people. With Secomea, you can manage your technicians' access with a few clicks, allowing them to intervene on any of your machines immediately, wherever they are. This minimizes response time, reduces security risks, and prevents downtime.



We help you handle third-party access: If you look at your factory floor, you might find that some of your appliances already have a Secomea gateway attached to them, provided by your machine supplier. Secomea has been empowering manufacturers and machine builders to secure cyber-physical systems for over 15 years: standardizing remote access for all stakeholders in the industrial ecosystem is integral to our company mission. With a single solution, we enable you to provide secure and controlled access to your vendors and easily monitor all of your internal and external remote access sessions.

We help you prevent cyber threats: At Secomea, cybersecurity plays a pivotal role. Secomea is an official CVE Numbering Authority (CNA), the first in Denmark. Our products are certified under IEC 62443-4-1 and IEC 62443-3-3, and our organizational security measures are based on ISO 27002 and certified in an ISAE 3402 report. Some of our features designed to meet the needs of the most security-conscious customers are privileged access management (i.e., hierarchy-based user roles/rights), activity logs, alerts setup, MFA, SSO via Azure AD and Okta, secure file transfer, and request for access.



We help you address the shortcomings of IT-centric tools: Our solution seamlessly connects to any OT/ICS machine (PLC, HMI, SCADA), no matter how old. That comes in handy if you are still using legacy equipment relying on serial communication. Secomea is easy to implement and easy to scale - it takes just one day to have it up and running on each of your production sites. The interface is very easy and intuitive to use, even for non-IT people, who can start using it right away without needing hours of training.

Why organizations opt for SRA solutions purpose-built for OT

Features	Traditional VPN	PAM solutions	Secomea's SRA
Zero-trust architecture	✗	✓	✓
Role-based access	✗	✓	✓
Least-privileged access	✗	✓	✓
MFA	✓	✓	✓
Secure file transfer	✗	✓	✓
Full audit log	✗	✗	✓
Direct access to PLC/HMI	✓	✗	✓
Low TCO	✓	✗	✓
Speed of implementation	✓	✗	✓

Secomea solution overview

Secomea Prime
Gain full oversight over your remote access sessions

IIoT Gateway
Connect hardware/ install software to any OT asset

IIoT Server
Seamlessly manage user access to assets

Access Client
Easy access to assets by authorized users

Fast implementation

- Plug-and-play for PLC, HMI, SCADA
- Full data tunneling support: UDP/TCP/USB
- Legacy equipment support: Serial connection/Layer2 communication

Easy user access and asset management

- Drag and drop user access management
- Advanced grouping for bulk management of user access rights
- Privileged access management with hierarchy-based user roles/rights

Smooth remote access to assets

- Request for access, on-demand access, scheduled access
- Supports all protocols: RDP, VNC, SSH, Telnet
- In-browser connection without installing plugin/app

Static tunnel connection

- No routing, firewall, or tunnel configuration required
- No dependency on static IP addresses and no problem with conflicting IP subnets
- Network traffic direction (Pull and/or Push) setup and port/IP restrictions

Security by design

- Login with MFA via SMS or SSO (Azure AD & Okta)
- Audit logs & Secure File Transfer
- Alerts and events setup with SMS/email alarms & automated actions

Smooth data collection

- Supporting OPC UA, Modbus TCP, Siemens S7, Ethernet/IP, MQTT protocols
- Configurable smart data aggregation, conditional sampling, and alarm generation
- Data delivery to third-party cloud service providers

About Secomea

Offices in Denmark (HQ), US, China, Japan

70+
Partner distributors

+9500
customers worldwide

+300.000
Gateways installed

CHR. HANSEN
Upfield
NOVARTIS
P&G
GEA
MOWI
TMEIC
We drive industry
MacArtney
UNDERWATER TECHNOLOGY
YASKAWA
Weil Technology

www.secomea.com