HONEYWELL
FORGE

REDUCE BUSINESS RISK AND ENABLE BUSINESS CONTINUITY WITH INDUSTRIAL GRADE REMOTE ACCESS

HONEYWELL INDUSTRIAL CYBERSECURITY

September 2020

TABLE OF CONTENTS

INTRODUCTION
MAKING REMOTE ACCESS MORE SECURE IN AN INCREASINGLY OPEN WORLD

> Industrial corporations face an ever-compounding challenge to manage and better secure remote access to their Operational Technology (OT) and industrial control systems (ICS) environment. While the requirements for compliance and proper governance demand that systems be protected from incidents that can hamper their operation, or compromise safety, solutions should not significantly impact operational costs.

With the world challenges of today, more and more companies are granting privileged remote access to their employees or trusted third-party service providers which often leave serious gaps that introduce significant cybersecurity risks. The frequent mismanagement of remote access is tantamount to inviting in ransomware, creating backdoors into industrial plants and manufacturing facilities responsible for producing chemicals, pharmaceuticals, energy, electricity, oil and gas utilities, metals and mining processing, food and beverage, water treatment and more. While summarily blocking this access might be particularly tempting for Chief information security officers (CISOs), its removal would, in most cases, lead to an acute loss in productivity, and a negative impact to incident response times.

Industrial corporations face an ever-compounding challenge to manage and better secure remote access to their Operational Technology (OT) and industrial control systems (ICS) environment. While the requirements for compliance and proper governance demand that systems be protected from incidents that can hamper their operation, or compromise safety, solutions should not significantly impact operational costs.

OT/ICS remote access cannot simply be viewed as an extension of standard IT remote access. OT/ICS assets, if compromised, pose extreme risk to the safety, integrity and efficiency of operations. With the potential for malicious, as well as accidental, incidents, it is crucial that corporate OT/ICS network managers work in partnership with their vendors, integrators and managed security service providers (MSSPs) to maintain compliance and vigilance. CIO/CISOs are accountable for cyber risk, requiring full control over the access details of every employee, vendor, integrator, or other third-party service provider requesting access to their networks, whether the source is internal or external, for local or remote access.

In this paper, we explore how industrial operators can allow safer and more controlled remote access to their OT/ICS. We examine how remote access has spiraled out of control to manage, maintain, standardize, their increasingly complex deployments. We will attempt to define the components for an Industrial Grade Remote Access solution which maximizes security, and through standardization and simplification it can reduce operations and maintenance (O&M) costs. This solution adopts a unique holistic approach, reducing the risk while maintaining the reward of remote access.

The paper challenges the conviction that traditional IT remote access (such as VPN and remote destop is sufficiently safe and secure for remote access to OT/ICS networks.

1 IIOT & INDUSTRY 4.0: THE PLETHORA OF RISKS AND REWARDS

Many CIO/CISOs struggle to balance the business benefits of IIoT and Industry 4.0 with the inherent security risks involved. Plants are becoming smarter and increasingly connected, increasing the dependence upon these technologies for business continuity. As the number of connected assets and machinery increases, the cybersecurity exposure expands, so will the need for a secure remote access platform that will enable the efficient and secure management of these devices.

When remote **connectivity risks are properly managed**, industrial companies can enjoy many extensive benefits.

WHY TAKE THE RISK AT ALL?

Smart manufacturing transforms businesses into proactive organizations that predict and fix potentially disruptive issues, optimize production on a frequent basis, evolve operations and satisfy customers, while increasing the bottom line. The transformation that it implies is huge. Figure 1 shows the predicted impact of IIoT and Industry 4.0 on businesses.

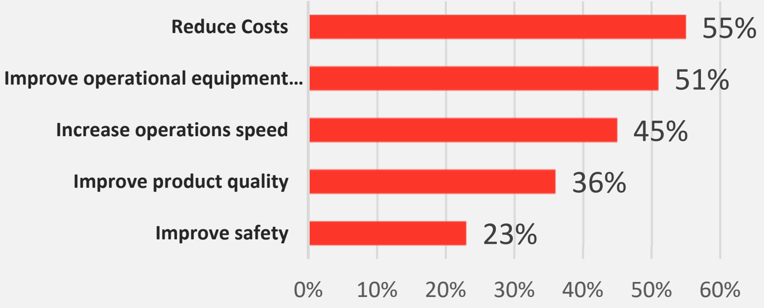


Figure 1: Benefits of Industrial IoT (Aberdeen Group)

BENEFITS OF REMOTE CONNECTIVITY

Technology should enable the business, that is the fundamental justification behind IIoT. At the same time, so too should remote access. With safer and more secure remote access to OT/ICS, an organization can realize the following benefits:

- **Maintain business continuity** – allow operations to continue, allow troubleshooting and maintenance to continue, without needing people physically onsite.
- **Keep staff safe or isolated** – the COVID pandemic has realized the importance of our people and the challenges that isolation or travel restrictions bring.
- **Enable remote workforce** – access experts on-call, manage assets from off-site, and augment site skills.
- **Improve incident response** – for both operational and cybersecurity events, allow responders to engage faster which in-turn reduces the severity of impact.
- **Eliminate travel time and travel costs** – avoid the travel scheduling delays to have experts onsite, as well as the flight/hotel/meal costs to bring experts to site.
- **Standardize and centralize** – see below:

Did you know, remote access can drive standardization and centralization? By reducing the variety and complexity of remote access solutions, it allows centralized skills and resources to support multiple sites at once. This includes a standardized approach for staff, contractors, integrators, and any trusted third-party service providers. It is important to recognize that remote access and connectivity is a powerful enabler of multi-site standardization and centralization of skills allowing support of global sites.

MULTIPLE TYPES OF REMOTE USERS NEED TO REMOTELY ACCESS ICS NETWORKS

Better securing access to industrial networks is no trivial task. Understanding operator roles can have a significant impact on how the remote access strategy evolves. In addition, the sheer number of remote connections must be managed in order to ensure that only authorized and supervised activities are happening in the operational domain. In most control systems, the roles that require remote access to control assets may include, but are not limited to:

- ✓ Plant security engineers
- ✓ System engineers
- ✓ Security specialists
- ✓ Operational and maintenance engineers
- ✓ Equipment vendors
- ✓ Project teams, including those in the midst of project delivery.
- ✓ Technical assistance centers (TAC) and help desk support
- ✓ System integrators or MSSPs

Complex industrial corporations often have tens or even hundreds of sites, each with hundreds to thousands of devices. Third-parties may be required to connect and access these devices at any given moment. The number and purpose of remote access sessions grows exponentially, given that every connected device has data to share, needs cybersecurity management, support, troubleshooting, maintenance, and security updates.

Due to the prohibitive costs associated with onsite vendor and integrator visits, many of these actions can best be performed centrally and/or remotely. The security risk to OT/ICS networks is ever-present; the greater the number of sites and OT/ICS assets, the greater the number of service providers, and the greater the need for a single, centralized remote access security solution.

Billions of smart devices are becoming connected: The number of connected smart devices was predicted in 2016 to reach 30 billion devices possible by 2020[1], that prediction held true and expected to continue explosive growth with billions of new devices each year[2].

[1] Syed Zaeem Hosain, Reality Check: 50B IoT Devices Connected by 2020, http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10

[2] Gilad David Maayan, IoT Rundown for 2020, https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

2 CHALLENGES TOWARDS THE HOLISTIC MANAGEMENT OF MORE SECURE REMOTE ACCESS

Notwithstanding IIoT’s tremendous potential, organizations must overcome numerous issues and challenges that are inhibiting IIoT’s growth, and in turn the industrial companies’ growth. The key hurdles that need to be addressed include the following.

MAINTAINING COMPLIANCE IN THE REMOTE ENTITY

Today, many industrial operators rely on project teams, integrators or vendors to maintain compliance with security policies and procedures for their own devices and assets, such as PLCs, HMIs, RTUs and others. However, industrial operators have very limited visibility or impact on the security compliance or standards of the vendors accessing their OT/ICS networks, and mainly rely on the self-reporting of the 3rd parties or ad hoc point-in-time assessments.

ENSURING VISIBILITY AND SECURITY MEASURES ON REMOTE ACCESS SESSIONS

Many industrial corporations do not even know how many devices are connected across their sites and plants, and the nature of these assets. Part of the security equation involves how operational assets are accessed and managed, and how the cyber security posture of a control system can be impacted if remote connectivity risks are not understood by a business, or is conducted poorly. A cybersecurity fundamental is to know your assets, and with the growth in connected things to the network, visibility needs to be comprehensive, up-to-date and automated. After all, unknown devices cannot be secured or backed up.

CYBERSECURITY IMPACTS IF OT/ICS IS COMPROMISED

Everyone is concerned about the risk and impacts to individuals as well as the organization if a cyber attack occurs. We rely on publicly disclosed information on cyber attacks to inform our decision on how much to invest in cybersecurity. This is a misleading source of information, as organization refrain from any public disclosure due to embarrassment and negative publicity and only a small percentage of actual cyber events are publicized.

From Honeywell's analysis[3] of cybersecurity attacks and their impacts on industrial operators, there are 3 main categories of loss.

DIRECT LOSS	INDIRECT LOSS	
IMMEDIATE CONSEQUENCES	**UNPLANNED LABOR**	**LONG TERM**
• Lost sales • Damage • Injury • Public health & safety • Release of energy or hazardous material • Non-compliance • Downtime • Reduced output or quality • Ransomware paid	• Inefficient manual workarounds and manual operations • Incident response and containment • Forced overtime and consulting • Post-incident recovery and rebuild • Validation and verification of known good	• Stock price and ratings • Investor and public relations • 3rd-party liability, contract commitments, and losses • Insurance and lending • CAPEX/OPEX project deferrals • Annual operating plan

Table 1: OT/ICS Cybersecurity Losses (Honeywell Cybersecurity)

As the table shows, there are many types of losses associated with an OT/ICS cybersecurity incident. The risks to the business are high and underscores the seriousness and gravity remotely connecting to OT/ICS.

Traditional IT remote access is intended to balance the risk and impacts to a business network compromise. However, the impacts of an OT/ICS compromise are much higher and therefore the cybersecurity safeguards need to be increased as well. As we continue in this paper, we will share what Industrial Grade Remote Access capabilities should be in place to make remote access safer and more secure.

BALANCING THE RISKS AND REWARDS OF REMOTE ACCESS

While IIoT offers huge value potential, organizations must overcome a multitude of issues, and learn to manage and secure IIoT's growing drive for connectivity in order to reap the benefits.

This is clearly a crucial issue for OT/ICS cybersecurity decision makers. The partial solutions and workarounds used today are not the right answer. What is needed is a single, centralized solution that mitigates risks and empowers businesses to forge ahead towards Industry 4.0.

[3] Honeywell, Exposing Cybersecurity Total Cost of Ownership, https://gateway.on24.com/wcc/eh/2360375/lp/2372910/exposing-cybersecurity-total-cost-of-ownership/

3 RESTORING ORDER TO INDUSTRIAL COMPANIES

Industrial companies have inadvertently opened up their remote network access to back doors from an array of employees, third parties, vendors, integrators and other service providers. The number of these parties seem to be multiplying at an uncontrollable rate. In many cases, network backdoors have been transformed into "revolving doors", introducing severe risks. In addition, there are significant multifaceted issues involved with enabling access by so many remote operators.

THE PATH FROM CHAOS TO CONTROL

The challenge to manage and secure the exponential number of connected entities is creating confusion and disorder. Many CISOs and OT security teams have been simply overwhelmed by the complexity of trying to manage so many disparate platforms and systems, and the differing needs of each third-party provider.

The steep business and technological challenges on the path to IIoT can be surmounted. Winning organizations will be those that master and hone the ability to manage a centralized platform for a diversity of devices and sensors. From there, organizations can apply more informed decision-making and operational efficiency to achieve new performance thresholds.

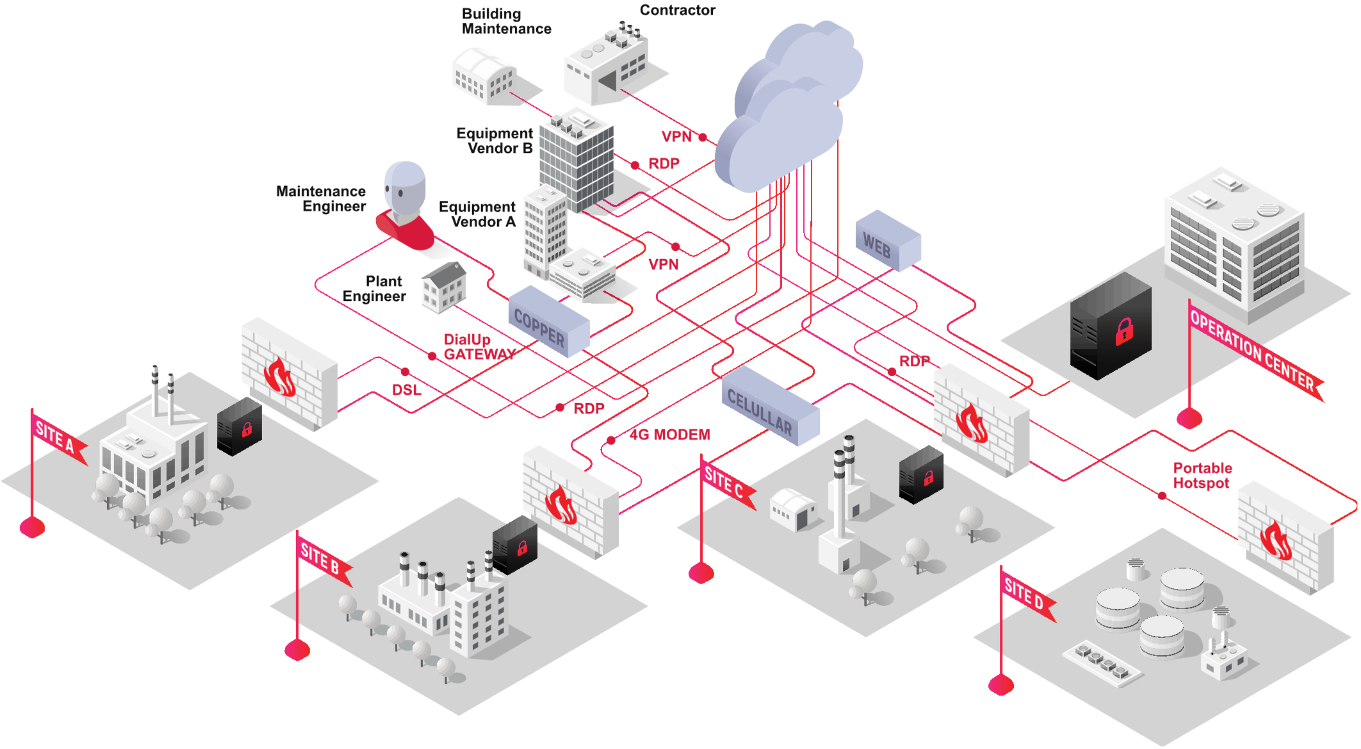


Figure 2: Multiple vendor connections to multisite corporation without a centralized remote access system

SHORTCOMINGS IN EXISTING SOLUTIONS:
WHAT'S NOT WORKING TODAY?

Outsourcing services does not relieve the CIO/CISOs of their responsibility to ensure that appropriate controls are in place to protect their assets, and prevent opening doors to malicious security vulnerabilities. And when multiple vendors and platforms connect remotely to the OT network, the latter needs to contend with multifarious issues and risks. The below list presents several inadequacies in current solutions, but is by no means exhaustive:

- **VPN is always-on, always-authorized, and connects threats on remote devices**
  Virtual private networking (VPN) typically gives full network access via a secure tunnel to a vendor or integrator that has been authenticated. In most cases, once authenticated, there is no way to prevent the vendor from viewing any asset or device on the remote operational technology (OT) network. There is no way of auditing sessions, and so remote sessions cannot be terminated, and a time-based policy, preventing remote access to a certain device during a certain time period is not possible. In addition, uncontrolled third-party devices and platforms can spread malware to an entire subnet or network that is made available through the tunnel.

- **Lack of role-based security**
  Once authenticated and authorized, an operator can do anything on the network and there is no way of knowing or controlling what operators do, or do not do. The inherent security and business risks associated with giving third-party operators unnecessary privileges include harm done to assets and data, as well as charges for work not performed. These issues may be malicious or unintentional.

- **Vendor-provided remote access platform are not necessarily secure**
  When a vendor has an inferior remote access platform, multiple inbound and outbound ports may have to be opened on the firewall. Asset owners should be aware that the vendor could be exposed to untrusted and hostile environments. A compromised vendor/operator machine could enable an attacker to piggyback on a trusted connection into the control system, unless additional zero-trust safeguards are in place.

- **Noncompliance of vendor's solution with corporate security policy**
  It is not uncommon for operations and engineering teams to deploy their own shadow infrastructures without the awareness of corporate security or IT. When the vendor's remote access solution does not comply with the company's security policy, there is a serious risk of a backdoor opening into the industrial site. Standards may even be lax to the point that passwords are stored on sticky notes on an operator's PC. When there are multiple vendors, this risk may increase exponentially.

- **Little accountability over the multitude of vendors**
  The lack of up-to-date audit data is an inherent hurdle in securing remote access to OT/ICS networks. It is challenging to track who logs on to a system, and when; the lack of supervision and recording mean that there is no real way to control or limit who can connect to a specific device, what activities are permitted to be performed, and stakeholders have practically no visibility into who is currently connected to their networks and assets.

4 A COMPREHENSIVE BLUEPRINT FOR INDUSTRIAL GRADE SECURE REMOTE ACCESS MANAGEMENT

Industrial operators are struggling to protect their highly complex multi-site and multi-vendor OT/ICS networks. Despite the great potential of IIoT to propel increased efficiency and associated cost savings, the growing surge in connected devices adds cybersecurity exposure.

This section describes Honeywell's best practices for managing OT/ICS remote access security in this era of industrial hyper-connectivity. The challenge is to provide a more secure, cost-effective solution based on known challenges and to mitigate the increasing risks associated with the rapidly evolving needs of industrial corporations.

#1 DEPLOY ONE CENTRALIZED, VENDOR-NEUTRAL, SECURE REMOTE-ACCESS SOLUTION

Enable expert skills located centrally, or anywhere in the world, to use a standardized solution to support multiple sites. Costs savings are derived by consolidating different remote access solutions at each site, and reducing the operations & maintenance costs by deploying one single, centralized platform for Industrial Grade Remote Access.

KEY REQUIREMENTS AND BENEFITS:

□ Reduce operations & maintenance costs
  ○ Reduce training and support staff
  ○ Eliminate duplicate multi-vendor products and increase negotiating leverage
□ Centralized authentication and granular controls
□ One solution for remote access and file transfers
□ Full audit trail of requests, authorizations, sessions, sites, users, endpoints, protocols, etc.

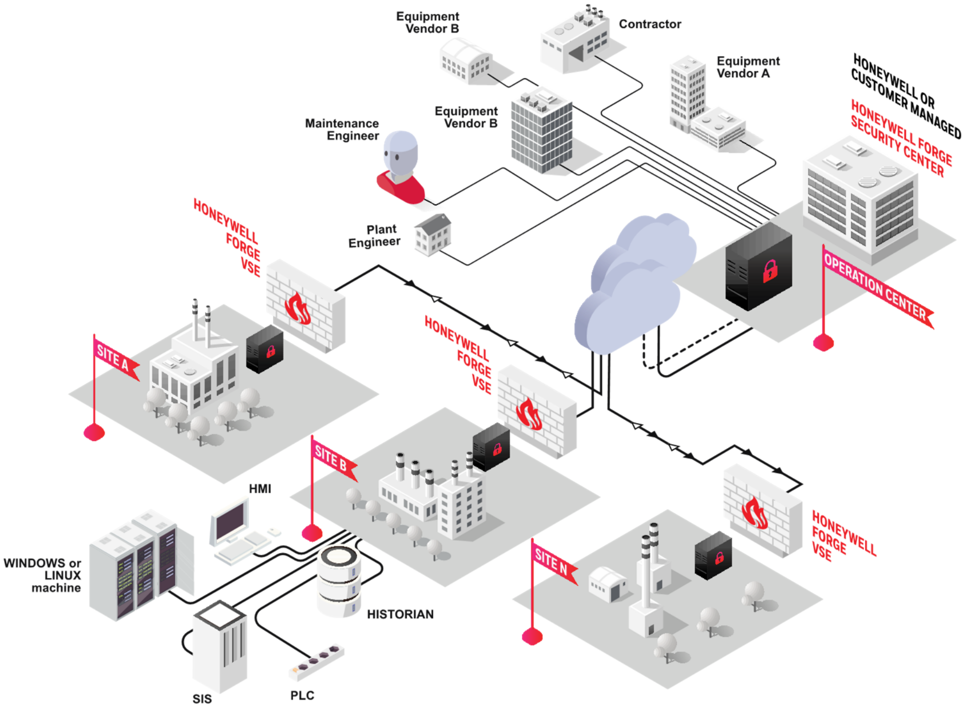


Figure 3: Centralized Multi-vendor Multi-site Corporation Industrial Grade Secure Remote Access system

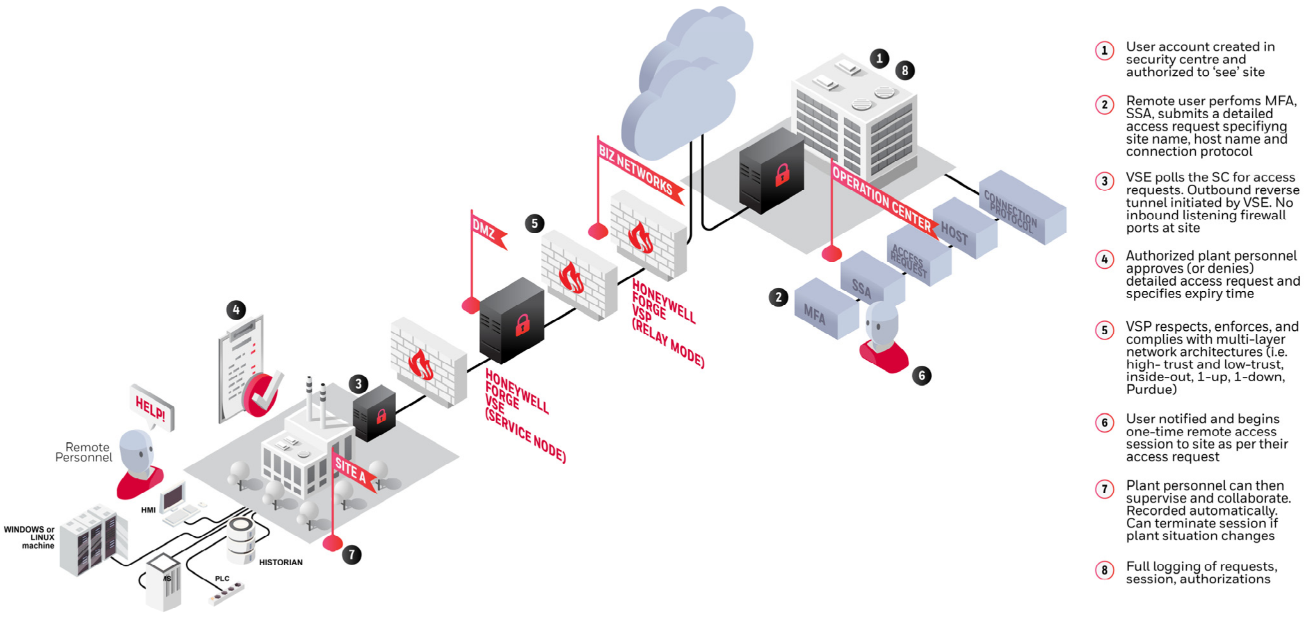
#2 REDUCE RISK WITH INDUSTRIAL GRADE SECURE REMOTE ACCESS CAPABILITIES

Remote access into corporate IT networks, is a different impact and threat level compared to OT/ICS remote access. The same approach should not be used, instead the cybersecurity safeguards for OT/ICS must be proportionate to the immediate and long-term impacts of OT/ICS to the business.

Ensure that remote access enables business productivity, not increased business risk.

KEY REQUIREMENTS AND RISK REDUCING SAFEGUARDS:

- ☐ No inbound firewall rules to ICS network. All connections are initiated from inside the high trust network by the VSE Service Node over a single outbound port (aka., reverse tunnel) to the Security Center. *No direct attack surface!*
- ☐ Users connect to an intermediary system, the Security Center, protecting the sites from direct connections or direct attacks.
  - ○ Comply with CIP-005-5 requirement R2, expecting an intermediary system between remote device and critical systems.
- ☐ Multifactor authentication compliance to Security Center; separate from local per-site authorization.
  - ○ CIP-005-5 requires encryption and multifactor authentication.
  - ○ ISA/IEC 62443-3-3 SR1.1(2) requires multifactor authentication.
- ☐ Easily conform to any multi-level multi-firewall network architecture and communication policy (e.g., de-militarized zones, Purdue model, one-up one-down)
- ☐ Site-controlled human authorization per session. Allowing site autonomy in addition to centralized user management.
  - ○ ISA/IEC 62443-3-3 SR1.13(1) requires explicit access request approval. Remote access should not be 'always on & always authorized'. It should only be possible when needed, after explicit authorization.
- ☐ Authorization is time-limited per-session, per-user, per-host, per-protocol.
- ☐ Remote user or remote computer is never part of trusted network. Cannot escape the point-to-point channel established across other networks. The point-to-point channel has one purpose and cannot be elevated or used for anything else.
- ☐ Real-time supervision (i.e., screen sharing), recording, playback, and session termination.
- ☐ Local authority to terminate sessions for unrecognized, suspicious, or plant operational situation changes (e.g., plant upset, incident response, emergency).
- ☐ Port Bridging: Single-port, machine-to-machine, device-level VPN tunnel
  - ○ Overcoming duplicate IPs, overcoming double NAT'ing, applications that do not support multiple firewall layers, does not have its own protocol security,
- ☐ "Hypertunnel" – point to point connection between a remote desktop, and a specific OT device through vendor and protocol agnostic communications
- ☐ Controlled environment for secure file transfer, patches and updates



1 User account created in security centre and authorized to 'see' site

2 Remote user perfoms MFA, SSA, submits a detailed access request specifiyng site name, host name and connection protocol

3 VSE polls the SC for access requests. Outbound reverse tunnel initiated by VSE. No inbound listening firewall ports at site

4 Authorized plant personnel approves (or denies) detailed access request and specifies expiry time

5 VSP respects, enforces, and complies with multi-layer network architectures (i.e. high- trust and low-trust, inside-out, 1-up, 1-down, Purdue)

6 User notified and begins one-time remote access session to site as per their access request

7 Plant personnel can then supervise and collaborate. Recorded automatically. Can terminate session if plant situation changes

8 Full logging of requests, session, authorizations

Figure 4: Honeywell's remote access connection and authorization process

#3 DEPLOY SOLUTION THAT IS FAST, EASY AND FLEXIBLE

When it is time to move ahead, technologies that are difficult to deploy add costs to deployment, as well as ongoing operations & maintenance costs throughout the lifecycle of the solution.

KEY REQUIREMENTS:

- ☐ Deploy as Customer hosted and managed, or a Honeywell hosted and managed service.
- ☐ Simple user experience. Quickly onboard and connect staff, contractors, and vendors.
- ☐ Transfer data and content securely to and from OT/ICS environments with Enterprise Threat Detection capabilities
- ☐ Remote access sessions conducted using VNC, RDP, HTTP, HTTPS, SSH etc.
- ☐ On the VSE Service Node, exists a Password Vault feature that holds the actual password; ensuring it is never revealed to the remote user or Security Center. Avoids the complexity of sharing passwords or changing them after each use or termination of access.

#4 ENTERPRISE SCALABILITY AND EXPANDABILITY

Rarely do organizations have all the budgets they need, or all their requirements defined, or ready to implement all security controls at the same time. Most often an organization makes incremental investments and improvements into their OT/ICS security program year over year. Selecting a solution that can easily scale across multiple sites, and expand features can save costs in the future and scale with the organization.

KEY REQUIREMENTS:

- ☐ Add sites, users, managed endpoints, and features as needed
- ☐ Avoid complicated or costly custom integration between different cybersecurity solutions.
- ☐ Available Expansion: Patch management, antivirus management, risk monitoring, compliance checking, hardening compliance, health & performance monitoring, and more
- ☐ Part of the Honeywell Forge Cybersecurity portfolio: Enterprise Threat Detection, Secure Media Exchange, Consulting Services, Managed Services, and more.

CASE STUDY

AN OIL AND GAS COMPANY (OG)

The case study below illustrates a deployment of a centralized, Industrial Grade Secure Remote Access solution.

THE PROBLEM

OG is one of the largest oil and gas companies in the world, with 40+ sites on four continents, and over 80 vendors connecting to plants on a daily basis. The company was aware of its high operational costs, and lack of control or visibility over what the many third-parties were, and were not, doing when performing their tasks. OG was looking for a solution to address three main areas:

- **Vendor accountability** - improving control over connecting vendors, including auditing, verification and supervision of all performed work
- **Securing remote access** - controlling access to all company sites, including site-controlled authorization, password control, centralized authentication, and asset visibility
- **Cost reduction** - as a derived benefit from a standardized and centralized solution

THE SOLUTION

OG deployed a remote access security solution that included the following components:

For third-party accountability (vendors, contractors, support personnel):

- Full audit
- Real-time supervision and session termination
- Remote access granted by plant personnel
- Remote access sessions conducted with Virtual Network Computing (VNC) or Remote Desktop Protocol (RDP)

For security:

- Granular authorization and privileges at the Center, as well as site-controlled authorization for each plant
- Plant security dashboard
- Deployed policies per plant
- Designation of access privileges per asset
- Management and control of remote access
- Continuous monitoring of field assets

RESULTS

A few weeks after deploying the solution, OG noted a productivity improvement (i.e., cost reduction) resulting from a decrease in required resources to follow up vendors' work, and manage the site connections. Vendors completed their work faster and thus had time to carry out additional tasks. The site managers reported that they had a much fuller picture regarding what was being done at their sites, and that the new solution handled unified plant security compliance, as well.

In summary, the solution, implemented across all plants, **saved over 35% in operational costs, and increased visibility, compliance and security dramatically**. It delivered its promise, and is currently being used across multiple sites daily.

5 CONCLUSION
SECURE REMOTE OPERATIONS AND ENABLE BUSINESS CONTINUITY WITH INDUSTRIAL GRADE SECURE REMOTE ACCESS

> "Industrial companies need a comprehensive, cost-effective solution for cybersecurity management and compliance. While there is an abundance of point solutions for each piece of the puzzle, there are very few solutions like Honeywell's that offer a comprehensive, unified solution for OT/ICS cybersecurity. This solution provides support from asset discovery to policy enforcement and monitoring, all the way to real-time protection. The solution provides industrial companies with multiple sites a fully integrated platform to easily manage and secure their operational their operational technology."
>
> **SID SNITKIN**
>
> VICE PRESIDENT AND GENERAL MANAGER,
> ENTERPRISE ADVISORY SERVICES, ARC ADVISORY GROUP

Companies around the world are facing growing challenges to ensuring their operations run without interruptions. Industrial Grade Secure Remote Access is a core solution, when setup properly, that can enable secure remote operations and business continuity from anywhere in the world. Industrial companies should take an uncompromising approach to their remote remotes access needs. Any solution should make remote access manageable and accountable. The solution must save company resources and lower operational cost and it should minimize the associated risks while enabling maximum benefit.

ABOUT
HONEYWELL INDUSTRIAL CYBERSECURITY

Honeywell has more than 100 years of industrial experience and over 15 years of industrial cybersecurity domain expertise. We are the leading provider of cybersecurity solutions, protecting the availability, safety and reliability of industrial facilities worldwide.

Industrial Cybersecurity Consulting

Managed Security Services

Integrated Cybersecurity Solutions

Cybersecurity Software

- Honeywell Forge
- Secure Media Exchange

Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting, and integrated security solutions. We combine industry-leading expertise in cybersecurity and decades of experience in process control, for the best solution in an operational technology (OT) environment. The Honeywell Forge Cybersecurity Suite provides an industrial-grade solution to secure remote access. Visit us at www.becybersecure.com to learn more.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 3030
www.honeywellprocess.com

WP-20-22-ENG | September 2020

Honeywell