LEARNING MADE EASY

eWON Special Edition

Secure Remote Access for Industrial Machines

for dummies®
A Wiley Brand

Learn the business benefits of remote access

Ensure secure access via Internet or cloud

Diagnose and solve problems remotely

Brought to you by:

eWON®

Jon Jacobsen

Lawrence Miller

About eWON

eWON is a product brand of HMS Industrial Networks, one of the leading independent manufacturers of products for industrial communication, including remote maintenance. HMS develops and manufactures solutions for connecting automation devices to industrial networks. The company markets its products under the brand names Anybus, IXXAT, and eWON.

Under the eWON brand, HMS offers four ways to remotely access and monitor industrial equipment:

- Remote Access
- Remote Data
- Remote Management
- Remote Networks

eWON remote solutions are the Internet of Things in its purest form. Equipping an industrial machine with an eWON product connects the machine to the Internet, giving users access to it anytime, anywhere.

In this guide, eWON leverages its years of experience to provide an in-depth look at the first solution — remote access.

Secure Remote Access for Industrial Machines

eWON Special Edition

by Jon Jacobsen and Lawrence Miller

for dummies®
A Wiley Brand

Secure Remote Access for Industrial Machines For Dummies®, eWON Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate

Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

ISBN 978-1-119-41339-4 (pbk), ISBN 978-1-119-41338-7 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Executive Editor: Katie Mohr

Business Development Representative: Frazer Hossack

Production Editor: Selvakumaran Rajendiran

HMS/eWON Special Help: Francis Vander Ghinst, Romain Borremans, Dominique Blanc, Blaise Ngung

Table of Contents

Introduction

After-sales service and support for industrial machines is often costly and time consuming. Experienced engineers and technicians often must travel to customer sites to diagnose issues, answer questions, provide training, and resolve problems. Wouldn't it be awesome — for you and your customers — if you could quickly and securely perform diagnostics and resolve most of those issues remotely?

About This Book

Secure Remote Access for Industrial Machines For Dummies, eWON Special Edition, consists of six short chapters that explore:

- What remote access is, how it has evolved, and the business benefits of remote access (Chapter 1)
- The basics of remote access environments (Chapter 2)
- How to ensure secure and reliable remote access over the Internet and in the cloud (Chapter 3)
- Secure remote access solutions from eWON (Chapter 4)
- Real-world remote access use cases for different industries (Chapter 5)
- How to get started with the eWON Cosy (Chapter 6)

There's also a convenient glossary at the end of the book, in case you get stumped on any technical acronyms or concepts.

Foolish Assumptions

In this book, we assume that you are an automation engineer or field technician working for a small or medium machine builder or original equipment manufacturer (OEM). Thus, while you no doubt have a strong understanding of the machines that you build or support, you aren't necessarily as comfortable with technologies such as the Internet, cloud computing, remote access, and information security. As such, this book is written primarily for "non-techie" readers.

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information you should commit to your non-volatile memory — along with anniversaries and birthdays!

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

TIP

Tips are appreciated, never expected — and we hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much we can cover in a short book, so if you find yourself at the end of this book, thinking "Where can I learn more?" just go to `www.ewon.biz`.

Where to Go from Here

Chapter 1 might be a good place to start. However, each chapter is written to stand on its own, so if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though we don't recommend upside down or backward)!

IN THIS CHAPTER

- Understanding why remote access is necessary
- Exploring remote access options — past and present
- Realizing the benefits of remote access

Chapter 1
Making the Case for Remote Access

In this chapter, you learn about the need for and benefits of remote access, the history, advantages, and disadvantages of different remote access technologies, and the many business and technical benefits of remote access.

Defining the Need for Remote Access

Perhaps for as long as industrial machine builders have existed, they've had the desire to look into the operation of their machines from afar. For original equipment manufacturers (OEMs) with far-flung fleets of machines at customer facilities, as well as for end-user manufacturing companies with multiple sites and corporate engineering centers, visibility into the operation of remote assets presents a compelling business case.

TIP

Typical use cases for remote access to industrial machines include:

- Troubleshooting and programming Programmable Logic Controllers (PLCs) remotely
- Viewing and controlling your remote Human Machine Interfaces (HMIs)

- Connecting to a web camera for assistance
- Supporting field technicians for commissioning

Exploring the Business Benefits of Remote Access

The ability to remotely access a machine's control system can help troubleshooting and solve an estimated 60 to 70 percent of operating problems, avoiding the need for support personnel to travel across town — or around the world. The types of problems that can derail production often don't require fixing the machine so much as tweaking its programming or other parameters. For example, you can accommodate changes in raw materials, machine wear, or other production inputs that may have shifted over time.

REMEMBER

Remote access enables you to move from a reactive support model to a proactive service model with benefits that include:

- Cutting travel costs (see Table 1-1)
- Improving responsiveness
- Reducing the impact of emergencies
- Optimizing engineers' workloads
- Maximizing machine uptime and productivity

TABLE 1-1 Out-of-pocket Costs for a "Quick" Site Visit

Description	Cost (USD)
Travel to local airport	$20
Airfare	$600
Rental car (three days)	$170
Hotel (two nights)	$285
Food and incidentals	$230
Parking (three days)	$30
Total (not including the cost of the engineer)	**$1,335**
Approximate cost of eWON Cosy	$500

Rapid issue resolution also means less downtime and a faster return to full production for the machine builder's customer. On those occasions when an in-person service call is required, remote visibility can help ensure that the person with the right skills, the right parts, and the right tools is sent — increasing the odds of a "fix on first visit" outcome. All this leads to a better customer experience and higher customer satisfaction.

The pressures driving industry to adopt remote access strategies have only intensified in recent years as industry faces the continued loss of subject matter experts to retirement. The expertise of those remaining must be stretched over a larger installed base of production machines that is often increasingly deployed globally. Machine builders are also recognizing the opportunity that remote access opens up for creating new, revenue-generating, proactive and preventive services that can be offered to their customers.

Overall, everyone is looking for more efficiency, which means less waste. Machine builders can achieve competitive advantages using remote access (see Figure 1-1) to serve more customers and reach new geographic markets, even without a local service setup.

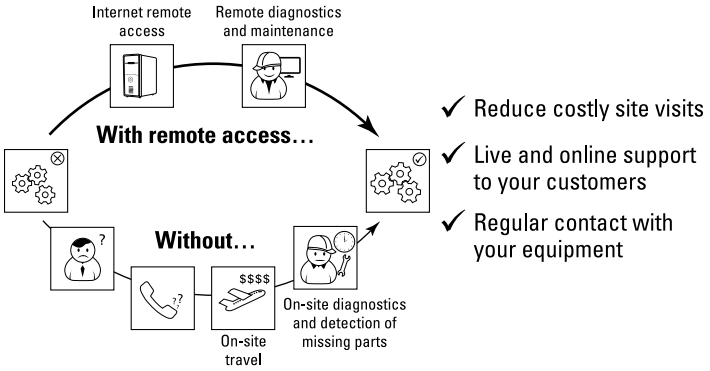

FIGURE 1-1: Achieve greater efficiency and competitive advantage with remote access.

Tracing the History of Remote Access

Early remote access to machines typically consisted of "out-of-band" management using a terminal console connected via an analog landline telephone and modem. These systems were slow, often difficult to install, and costly to operate and maintain.

Still, remote access through a modem connection continues to be popular today, aided by the availability of high-speed cellular networks. The main appeal of this remote access method is the ability to access controller data and bypass the customers' corporate network. Wireless modems that communicate via cell phone providers' data networks are available from many suppliers of programmable controllers.

This approach avoids the need for a wired phone line or the need to tap into the corporate IT network, though wireless signal availability in production areas can be an issue.

Further, working with a cellular network provider introduces its own complexities. Subscriber Identity Module (SIM) cards with fixed IP addresses cost extra and take time to acquire and configure. This approach entails ongoing network access and usage fees that can quickly add up — an expense that most machine builders would prefer to avoid, especially if continuous connectivity is not necessary.

Leveraging the Internet

A better means of remote machine access is to leverage the Internet and cloud computing technology. The primary challenge in this scenario is to securely manage the machine's connection to the end-user's corporate network and, in turn, to the Internet. Most companies' IT departments are understandably loath to grant blanket network access to non-employees for security reasons.

On-demand remote access

In remote asset management, where the ability to control the asset is essential, permanent access to the asset is necessary. Machine builders, however, do not always need permanent connections. Indeed, remote access for machine troubleshooting, maintenance, or service can be provided by an on-demand connection.

Why is this capability important? First, the end-user may want to prevent continual remote access to the machine. Disconnecting the machine from the LAN is not essential for security, but it gives the end-user physical control over when the machine is accessed and for how long. In this situation, the machine is ordinarily disconnected from the local area network (LAN). The

machine is connected only when necessary or when requested by the machine builder.

In addition, when remote connectivity is based on a volume-dependent pricing option, such as cellular technology, it can be desirable to establish the connection and pay only when necessary.

Outbound connections

Virtual private networks (VPNs) are an excellent solution from a technical standpoint, but allowing proper inbound network access while ensuring security can be a complex task. Every automation vendor typically uses a different set of network ports, and negotiating a clear path through a customer's firewalls requires careful configuration and sometimes delicate negotiations with resistant IT departments. By relying on an outbound connection across the factory LAN, you can resolve many firewall issues right off the bat. Indeed, if no incoming connections are made, no ports must be enabled in the corporate firewall for incoming connections, and no IT or firewall changes are needed to establish communication.

Software-based solutions

Using the Internet, a supervisory local PC can be remotely accessed and controlled using Virtual Network Computing (VNC)-like technology or other PC-based remote access software. In this scenario, software replicates and cedes control of the remotely accessed operator interface computer. Although this type of solution may be acceptable for remotely connecting to a PC, it potentially provides the user with access to the entire network — which is not acceptable, especially from a security perspective.

This approach presumes that there is an industrial PC that can run the application on the remote machine. This hardware and software entails additional expense, making its total cost of ownership higher than that of a dedicated device.

Router-based VPN solutions

Another solution is to rely on an on-demand VPN connection using an industrial router and a cloud-based management infrastructure. A Secure Sockets Layer (SSL) VPN connection typically presents few issues for a customer's IT department.

This method is even more interesting from a security point of view because it automatically adds a logical network segregation between the machine and the factory LAN. This configuration ensures that the remote engineer has no access to the factory LAN and can reach only those devices that are connected behind the remote access router. Machine builders can manage fleets of machines through a single secure interface. End-users, meanwhile, can use the platform to manage remote access rights with multiple OEMs. Therefore, this solution is the one we focus on in this book.

IN THIS CHAPTER

- Working out the details of computer networking
- Tracing the history of the Internet and the cloud
- Reviewing industrial network protocols

Chapter 2
Looking at Remote Access Environments

In this chapter, you learn the basics about computer networking technology, the Internet, and cloud computing, as well as Programmable Logic Controllers (PLCs), automation, and Human Machine Interfaces (HMIs).

Everything You Ever Wanted to Know About Networking

Chapter 1 describes the use of a router-based virtual private network (VPN) solution for remote access with a remote engineer accessing devices connected behind the remote access router. These devices usually connect on their own local area network (LAN), which is typically referred to as the "machine" LAN. A LAN is a computer network that operates across a relatively small geographic area, such as a building or factory or, in this case, an industrial asset such as a machine. A wide area network (WAN) connects multiple LANs and other WANs over a relatively large geographic area. The Internet is an example of a very large WAN.

LAN devices in machines such as programmable logic controllers (PLCs), panels, human machine interfaces (HMIs), computers, and other automation devices (for example, peripheral input/output equipment and drives) are typically connected via hubs or switches using Ethernet cables (*wired* connections). The most common LANs use the Transmission Control Protocol and Internet Protocol (TCP/IP) to communicate with other devices and networks. Every device on a TCP/IP network must have a unique IP address. The current version of IP (IP version 4) uses a 32-bit numeric address that is divided into four octets, for example: 5.39.46.101 (see Figure 2-1).

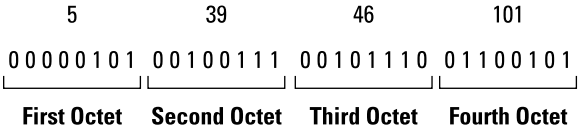

FIGURE 2-1: An IP address consists of 32 bits of information, divided into four 8-bit sections known as "octets."

An IP address represented in binary notation (see Figure 2-1) consists of 8 bits that are set to either a 1 ("on") or 0 ("off") and arranged into four groups, known as "octets," with the following values from left to right in each octet, as follows:

- The first bit is equal to 128 ("on") or 0 ("off")
- The second bit is equal to 64 ("on") or 0 ("off")
- The third bit is equal to 32 ("on") or 0 ("off")
- The fourth bit is equal to 16 ("on") or 0 ("off")
- The fifth bit is equal to 8 ("on") or 0 ("off")
- The sixth bit is equal to 4 ("on") or 0 ("off")
- The seventh bit is equal to 2 ("on") or 0 ("off")
- The eighth bit is equal to 1 ("on") or 0 ("off")

In this way, any whole number between 0 and 255 can be represented with a 32-bit IP address by adding together the binary result in each octet. For example, in Figure 2-1, the first octet is equal to 5 because only the sixth and eighth bits are "on," so the result is 0+0+0+0+0+4+0+1. The second octet is equal to 39 because the third, sixth, seventh, and eighth bits are "on," so the result is 0+0+32+0+0+4+2+1. See whether you can apply this logic to obtain the values in the third and fourth octets of Figure 2-1.

Every computer or other IP device uses an IP address, but it also uses a subnet mask and usually a gateway.

The *subnet mask* is a 32-bit address (like the IP address) that *masks* the IP address to compute the network address. Computers use a subnet mask to know whether a recipient IP address belongs to its network or not. If the computer and the recipient IP address belong to the same network, they can communicate to each other directly. If they don't, they must communicate through the gateway.

The *gateway* is a device that has two or more IP interfaces and handles the connections between two or more networks. For example, eWON Cosy is a gateway.

In Figure 2-2, Device A must communicate with Device B. Both devices belong to the same physical network, but the devices don't know that. They must compute it from the IP address and the subnet mask. Device A uses the IP address 10.0.0.67 and the subnet mask 255.255.255.0. Masking 10.0.0.67 and 255.255.255.0 produces the network address 10.0.0.x. This means that any device using an IP address that starts with 10.0.0, such as Device B, belongs to Device A's network and thus can communicate with Device A directly.

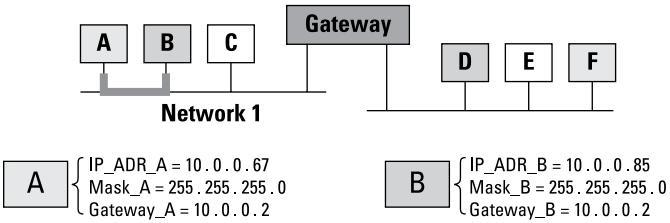

FIGURE 2-2: Two devices communicating within the same network.

In Figure 2-3, Device A needs to communicate with Device E. However, Device E does not belong to Device A's network because its IP address is 10.**1**.0.19. This means Device A must pass the message to the gateway, which in turn forwards it to Device E.

In both figures, the gateway has two connections. Each connection has an IP address that belongs to the network to which it is connected.

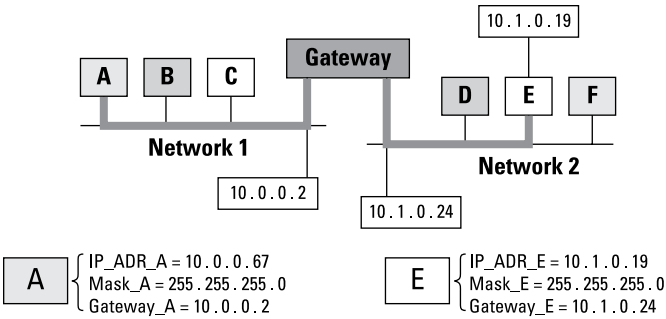

FIGURE 2-3: Two devices communicating on different networks.

REMEMBER

Each automation device connected on the machine LAN must have a unique IP address.

For remote access, the machine LAN must be connected to the factory LAN (usually called the "WAN" in remote access terminology) using a router (see Figure 2-4). A router is a device that connects a LAN to another LAN that has a different network address portion. Because remote access occurs over the Internet, the WAN must be capable of reaching the Internet, typically through a factory router or firewall.

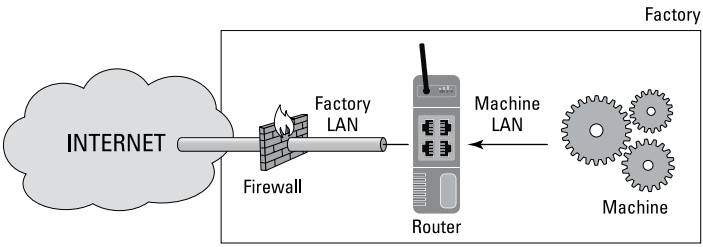

FIGURE 2-4: Connecting a machine LAN to the factory LAN with a router.

A limitation of the current version of IP is that there are only a little over four billion possible unique IP addresses. To temporarily get around this limitation, private IP addresses can be assigned to devices on the machine's LAN. However, private IP addresses cannot be routed across the Internet so they must be translated to a public IP address, using a process known as *network address translation (NAT).*

Network address translation (NAT) maps private IP addresses to public IP addresses for outbound traffic to the Internet. NAT is usually performed by a router.

TECHNICAL STUFF

Three ranges of private addresses typically are used for connecting devices inside a LAN:

- **Range 1:** IP addresses from 10.0.0.0 to 10.255.255.255 where the first number (10) represents the network portion of the address and the last three numbers represent hosts on that network (more than 16 million devices can be assigned as hosts; used in very large networks).
- **Range 2:** IP addresses from 172.16.0.0 to 172.31.255.255 where the first two numbers (172 and 16 through 31) represent the network portion of the address and the last two numbers represent hosts on that network (approximately 1 million devices can be assigned as hosts; used in medium to large networks).
- **Range 3:** IP addresses from 192.168.0.0 to 192.168.255.255 where the first two numbers (192.168) represent the network portion of the address and the last two numbers represent hosts on that network (approximately 65,000 devices can be assigned as hosts; used in small to medium networks).

The worldwide supply of unique IP version 4 addresses was exhausted in 2016. Many organizations are increasingly transitioning to IP version 6, which uses a 128-bit hexadecimal address and provides 3.4×10^{38} unique IP addresses — that's more than 340 undecillion (yes, that's a real number).

Exploring the Internet and Cloud Computing

In the 1960s the U.S. Department of Defense Advanced Research Project Agency (DARPA) developed ARPANET, the first packet switching network — and the precursor to the modern Internet.

The Transmission Control Protocol (TCP) was created in the late 1970s, followed by the Internet Protocol (IP). TCP/IP enabled ARPANET and other networks around the world to connect to each other. In the late 1980s, this network became known as the Internet.

Today, the Internet (and the World Wide Web) is ubiquitous, connecting networks and devices to vast amounts of information and resources around the world. For Millennials, it's practically a basic life necessity!

In 2006, Amazon officially launched Amazon Web Services (AWS) — and the "cloud" was born, uh, formed. Other major cloud service providers include Microsoft Azure, Oracle Cloud, Google, and IBM.

So, what exactly *is* the cloud? When the Amazon engineers conceived it, the *cloud* referred to all the networking "stuff" that happened behind the scenes to connect a LAN to the Internet — typically represented as a cloud in network architecture diagrams.

However, more specifically, cloud computing, as defined by the U.S. National Institute of Standards and Technology (NIST) is comprised of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Common cloud service models include:

- **Software as a Service (SaaS):** Customers are provided access to applications running on a cloud infrastructure but the customer has no visibility into, and does not manage or control, the underlying cloud infrastructure (for example, Google Gmail).
- **Platform as a Service (PaaS):** Customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no visibility into, and does not manage or control, the underlying cloud infrastructure (for example, IBM Bluemix).
- **Infrastructure as a Service (IaaS):** Customers can provision processing, storage, networks, and other computing resources and deploy and run operating systems and applications, but the customer has no visibility into, and does not manage or control, the underlying cloud infrastructure (for example, Amazon Web Services).
- **Connectivity as a Service (CaaS):** Customers get effective inter-network connectivity with flexibility and expandability that small and medium-sized businesses can afford, without the need to pay premiums or manage relationships with multiple providers (for example, eWON Talk2M).

TIP

You can think of the Internet as a route and the cloud (as well as the World Wide Web) as destinations on the Internet.

Connecting Automation Devices Other than Ethernet

Many industrial protocols are in use today, reflecting the highly specialized and varied range of industrial applications. Unfortunately, many of these protocols are proprietary, non-standard protocols developed for specific devices or functions. As a result, interoperability is often a challenge in today's connected industrial world.

Fortunately, most automation devices today are equipped with Ethernet ports. Automation/PLC protocols (such as those listed in table 2-1) are therefore transparently conveyed through the router, thanks to TCP/IP. But what about legacy automation devices that are not equipped with an Ethernet port? They usually come with a serial interface matching the RS232 or RS485 serial protocols. To remotely access them, the LAN/WAN router ideally should also play the role of a protocol gateway, converting the Ethernet protocol into a serial counterpart. An automation router therefore should be capable of embedding the protocol gateway functionality and supporting all the protocols listed in Table 2-1.

TABLE 2-1 Supported PLC Protocols

PLC Brand	Serial	Ethernet
Allen Bradley — Rockwell Automation	DF1	Ethernet/Industrial Protocol (EIP)
Siemens, VIPA	MPI/Profibus	ISOTCP
Schneider	Modbus/Unitelway	Modbus
Omron	Fins Hostlink	Fins TCP/UDP
Mitsubishi	Programming Protocol	MC Protocol
Hitachi	H-Protocol	H-Protocol

PLCS' FAMILY HISTORY

Although PLCs are common in many industries today, the first PLCs were invented for American automobile manufacturers. Previously, carmakers controlled their manufacturing processes with a variety of hard-wired relays and timers. These old-school devices got the job done, but every time a manufacturing process was redesigned, thousands of them had to be rewired — a costly and time-consuming task.

In 1968, General Motors' automatic transmission division sought proposals for a new way to handle changes in production processes. A Massachusetts company, Bedford Associates, won the GM contract and developed the first PLC, known as a Modular Digital Controller (Modicon). *Manufacturing Automation* has termed Dick Morley, one of the developers of the first Modicon, the "father" of the PLC.

Early PLCs used *ladder logic,* a programming method based on the circuit diagrams of the analog devices that the PLCs were replacing. Today's PLCs can be programmed in many different ways, but their purpose is still to provide reliable, programmable control of manufacturing processes.

IN THIS CHAPTER

- Looking at the dark side of the Internet
- Learning about firewalls and VPNs
- Choosing a web-hosted architecture
- Taking a "defense-in-depth" approach to security

Chapter 3
Ensuring Security and Reliability

Although the Internet enables remote access to networks and machines around the world with many business benefits, it also affords an opportunity for malicious activity — *cyberattacks* — that have become all too common today. In this chapter, you learn the basics of Internet security and how eWON protects your machines and data with its Talk2M defense-in-depth security architecture.

Surveying the Modern Threat Landscape

Large security breaches, typically involving credit card fraud and identity theft are frequently reported in the news, but there's a far more menacing — and potentially more devastating — threat of cyberattacks against critical infrastructure and machines such as public utilities, emergency systems, building environmental controls, and industrial equipment.

The 2013 data breach of U.S. retailer Target was the result of an attacker compromising Target's corporate network via a connected heating, ventilation, and air conditioning (HVAC) maintenance system.

Hacker groups motivated by a political or social cause may also try to damage industrial machines connected to the Internet. Perhaps the most significant threats arise from nation-states that may attack machines to achieve various objectives.

For example, the Stuxnet worm, identified in 2010, is believed to have been developed by one or more nations targeting Iran's nuclear program. The worm infected vulnerable programmable logic controllers (PLCs) and Siemens Step7 software at Iran's Natanz nuclear facilities, causing centrifuges to rotate at variable speeds to induce excessive vibration and destroy the centrifuges.

Thus, security must be "top of mind" for all machine builders, original equipment manufacturers (OEMs), and system integrators looking to remotely connect to their customers' machines over the Internet.

Understanding Firewalls and Virtual Private Networks (VPNs)

Firewalls control the flow of traffic between networks, such as a local area network (LAN) and the Internet. A firewall is typically installed at the perimeter of the network that it protects, and may consist of a hardware appliance, software, or a combination of hardware and software.


TIP

You can think of a *router* (discussed in Chapter 2) as the entrance to a medieval castle, and the firewall as the drawbridge at the entrance that controls access to the castle.

Although many advanced firewall designs and technologies exist, the basic operation of a firewall is to filter all inbound traffic from an untrusted network (such as the Internet) based on a set of configured rules.

By default, all *outbound* traffic from the trusted network is allowed — for example, from the LAN to the Internet. Inbound traffic that is sent in reply to an active outbound connection is dynamically permitted. For example, if a PC user on a corporate LAN opens a web browser and goes to `www.ewon.biz`, the inbound eWON web page traffic will be automatically allowed through

the firewall in response to the request initiated by the PC's web browser.

However, all *inbound* traffic that is not explicitly associated with an outbound request is blocked by default. To allow certain inbound traffic from the Internet, firewall rules must be configured to allow the specific type of traffic, from a specific source to a specific destination.

While a firewall protects the systems (including machines) and data on a LAN from unauthorized access, it does nothing to protect the confidentiality and integrity of traffic traversing the Internet on its way to and from the LAN. That's the role of a virtual private network, or VPN.

VPN technology provides encryption and tunneling functions for networked traffic across the Internet. Data is encapsulated in an IP "wrapper" that travels over the Internet. When data is sent, it must be wrapped and encrypted by a gateway using an encryption algorithm. At the other end of the communication link, the destination gateway must "unwrap" the data, decrypt it, and route it to its destination.

Why Use a Web-Hosted Architecture?

How do you establish VPN communication between your PC (the user) and the router on the machine side? You could install a hardware or software component on your PC to serve as the endpoint of the VPN tunnel that is initiated by the machine. For example, you could install a *VPN server,* a software application that manages all incoming VPN connections from various machines. This method requires installing and configuring the VPN server software on a PC, which isn't always straightforward and often requires specialized IT knowledge and skills. However, an advantage of this setup is that once the VPN server has been configured, the machine builder should only have to worry about maintenance activities, not IT issues. With a server application, users can connect to the same servers as the machine, and the VPN server is responsible for establishing the link between the user and the machine (see Figure 3-1).

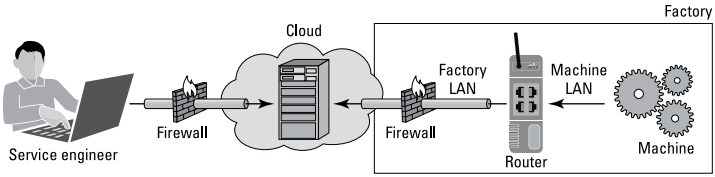

FIGURE 3-1: Using a VPN server to securely connect to your remote machines.

However, if the VPN server is hosted by an independent organization in a cloud as a Software as a Service (SaaS) offering (discussed in Chapter 2), it can be shared among several machine builders, each having a private account, and they can individually configure their users and machines. This solution reduces the web infrastructure cost for individual machine builders and OEMs, and can spread the cost over several machine builders.

A cloud-based architecture inherently provides better scalability than a pure hardware architecture based on hardware gateways or internal software applications. In fact, the web architecture can provide a load balancing function to distribute the number of necessary VPN connections or tunnels over several servers. It can also provide redundancy to ensure the resiliency of the remote access services in the event of a business disruption or disaster.

Looking at eWON Remote Access Layered Security

One of the key challenges with remote connections to industrial control systems is balancing the needs of an engineer or PLC technician with the mandate by the IT department to ensure network security, integrity, and reliability. Finding a solution that is readily accepted by both business groups has been a challenge for many years and a source of frustration and inefficiency for all stakeholders. Maintaining network security is essential for IT acceptance. At the same time, users will never use solutions that are complex, difficult, or hinder productivity. By focusing on both security and ease of use, eWON has created a remote access solution that works for both end-users and IT managers.

Security and reliability are two critical aspects of the Talk2M cloud. The Talk2M cloud is built on a "defense-in-depth" strategy,

which uses multiple security countermeasures across multiple layers of security controls (see Figure 3-2). The purpose is to protect the integrity of the Talk2M connectivity and information system. It is based on numerous industry publications, guidelines, best practices, and established security standards including:

- *ISO/IEC 27001 (International Organization for Standardization and International Electrotechnical Commission)*
- *U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*
- *Open Web Application Security Project (OWASP)*
- *Open Source Security Testing Methodology Manual (OSSTMM)*

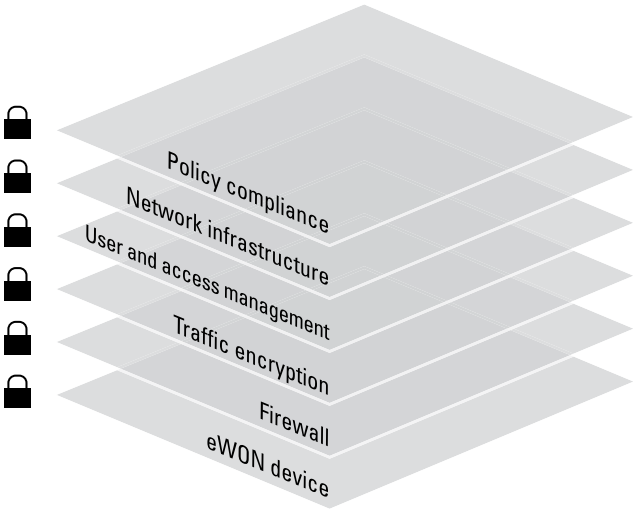

FIGURE 3-2: eWON's defense-in-depth strategy.

REMEMBER

From the hardware devices to the policies and procedures, security is a core competency fully integrated at every level within the framework of eWON solutions.

The different layers of eWON's defense-in-depth strategy are comprised of:

- **eWON device:** Users must be authenticated and have administration rights. Traffic on the machine/LAN side is

segregated from the WAN/customer side and users can access only authorized devices on the LAN. Specific controls include:

- *Network segregation*: The industrial routers are typically installed in the machine control panel with the machine connected on one side (LAN) and the factory network on the other (WAN). When a connection needs to be established, the eWON device acts as a gateway through which all traffic passes. When the eWON is first configured for VPN access, security settings on the device restrict traffic between its two network interfaces. This network segregation limits remote access to only the devices connected to the LAN of the eWON. Access to the rest of the network is prevented.
- *Device authentication:* The eWON routers themselves have user-level access rights separate from the Talk2M login. Only users with appropriate credentials and access rights can change the security settings on the eWON. Similarly, for the devices with data services, only authorized users can view or modify the data.
- *Physical key switch:* All eWON hardware devices feature a digital input. A switch can be connected to this input and the state of the switch can enable or disable the WAN port. This allows the end-user to keep full local control of whether or not the device is remotely accessible.
- *IP assignment and control:* The eWON needs the same type of settings as a PC connected to the same network (IP address, subnet mask, and gateway, plus any optional proxy settings). The eWON can be configured to receive those settings automatically via the dynamic host configuration protocol (DHCP). However, the eWON also can be set up to use a static IP address that is assigned and controlled by the IT department, if preferred.

» **Firewall:** Within the eCatcher application, Talk2M account administrators can set filtering and firewalling rules about which devices behind the eWON are remotely accessible and even over which ports (such as Ethernet, USB, or serial) and with which protocols they are accessible. Talk2M provides four different firewall setting rules based on declared devices' IP, ports, gateways, and eWON services access. From least restrictive to most secure firewall levels, they are:

- Standard
- High
- Enforced
- Ultra

When combined with Talk2M's user rights management, administrators can tailor the remote access rights to selected groups of users.

- **Encryption:** Communications between the remote user and the eWON are fully encrypted using the secure sockets layer (SSL)/transport layer security (TLS) protocol, thereby ensuring data authenticity, integrity, and confidentiality. All users and eWON units are authenticated using x.509 SSL certificates, and end-to-end traffic is encrypted using strong symmetric and asymmetric algorithms.
- **User management and accountability:** A Talk2M account can have an unlimited number of users. For every user who needs to access equipment remotely, administrators can create unique logins. This makes it easy to grant and revoke access privileges when needed. In addition, Talk2M account administrators can restrict which remote eWONs particular users can access, which services behind those eWON are accessible, and even the ports on those devices and the communication protocols used. For example, an administrator might permit remote users to reach the web services in a particular device for monitoring purposes but limit the ports used for making programing changes to only specific engineers. Controls include:
  - *Role-based access control (RBAC),* which defines which users can have access to which machines and allows different access levels
  - *Unique user logins with custom password requirements* (such as minimum length, letters, numbers, and special characters, expiration period, and unique password history)
  - *Multi-factor authentication (MFA),* which requires users to enter a one-time short message system (SMS) text code after entering their username and password
  - *Audit trail and logging activities* for each device to know who has connected, when, and for how long

TECHNICAL STUFF

- **Talk2M network infrastructure:** eWON regularly assesses the Talk2M architecture as part of its risk management framework. Appropriate controls are implemented for maximum security effectiveness and compliance with applicable regulatory requirements.

  eWON is contracted with several hosting companies that meet the following requirements:

  - *Globally redundant Tier 1 hosting partners:* To increase reliability, improve redundancy, and reduce latency, eWON works with multiple hosting partners throughout the world.
  - *24/7/365 monitoring:* The network of servers is monitored around the clock to ensure maximum availability and security. Monitoring makes use of intrusion detection systems (IDS) and host intrusion prevention systems (HIPS), as well as an array of alerting mechanisms.
  - *Certified data centers:* Relevant certifications include Service Organization Control (SOC) 1/Statements on Standards for Attestation Engagements (SSAE) 16/ International Standard for Assurance Engagements (ISAE) 3402, SOC 2, and International Organization for Standardization (ISO) 27001/27002/27017/27018.
  - *Cloud Security Alliance (CSA) corporate member:* eWON works with hosting partners that are corporate members of CSA, such as Rackspace and Softlayer.

- **Policies and procedures:** The Talk2M remote access solution is designed to be compatible with customers' existing security policies. By using outbound connections over commonly open ports (for example, 443 and 1194) and by being compatible with most proxy servers, the eWON router is designed to be minimally intrusive on the network and work within existing firewall rules. Talk2M account administrators can customize password policies to enforce compliance with corporate policies and can restrict which users can access which devices remotely. Talk2M account administrators can also use the Talk2M connection report to see which users are connecting to which devices and when, and verify that corporate remote access policies are being followed.

To provide the best possible business continuity, two service offerings are available to customers:

- **Talk2M Pro** is a "mission-critical" paid service offered with a service-level agreement (SLA).
- **The Talk2M Free+** provides full-featured free connection services with limited SLA guarantees.

The mission-critical Talk2M Pro service is designed to provide 99.6 percent uptime.

To provide these two levels of service, the Talk2M architecture is reinforced by several policy and control objectives including:

- **Hosting provider SLAs:** Mission-critical Talk2M Pro services are hosted through globally redundant Tier 1 hosting partners, which provides a 99.99 percent Internet access uptime (approximately four minutes of unplanned monthly downtime) and maximum server downtime of one hour. For Talk2M Free+ services, multiple hosting partners are used, typically providing 99 percent uptime.
- **Information system acquisition:** Key performance indicators (KPIs) of all servers are monitored, and all acquired information is displayed on a monitoring dashboard and logged on an alarm server for eWON's 24/7/365 staff.
- **Server rollout:** Multiple hardware providers ensure that VPN connections can be quickly rolled out from one VPN Server (VS) to another in the case of a major server failure.
- **Continuous monitoring services:** TalK2M services are continuously monitored by on-duty engineers.

Finally, to reduce network latency, data center sites are located on five continents (North America, Europe, Asia, Africa, and Australia) and eWON continues to expand into other regions. Low latency is required by some industrial programmable logic controller (PLC) protocols that are designed with small-sized Transmission Control Protocol/Internet Protocol (TCP/IP) packets. These protocols are much more sensitive to timeouts resulting from slow Internet connections and long distances between users and their machines. eWON routers can dynamically connect to the geographically closest, lowest load or the best performing VS to optimize performance and reduce latency.

SAVING THE WORLD — AND MORE

Thanks to Talk2M, users have avoided an incredible amount of support site travel, saving massive carbon emissions by using millions of VPN connections.

eWON devices are currently used in 156 countries around the world (see the accompanying figure).

Talk2M has even saved some marriages! Wonder how many? Check out real time facts and figures at `www.talk2m-live.ewon.biz`.

eWON routers located all over the world.

IN THIS CHAPTER

- Introducing eWON Cosy (remote access router)
- Getting your machines connected to the Internet and Talk2M
- Using eCatcher to connect your PC to Talk2M
- Communicating across a VPN connection
- Learning about other eWON remote access solutions and tools

Chapter 4
Understanding the eWON Remote Access Solution

In this chapter, you learn how to use eWON's flagship remote access solution.

Introducing eWON Cosy

The eWON Cosy is an industrial remote access router that is designed to offer easy remote access, across the Internet, to machines and installations at customer sites or in the field.

More explicitly, with eWON Cosy, machine builders, original equipment manufacturers (OEMs), and system integrators can troubleshoot machines, debug the Programmable Logic Controller (PLC) program, upload projects, gain remote use of a Human Machine Interface (HMI) or an IP camera without going on site, thus drastically reducing support costs.

eWON Cosy users are typically service or automation engineers who need access to machines installed at various customer locations, often spread over large geographic areas or even across the world.

How eWON Cosy Works

The eWON Cosy router establishes a secure virtual private network (VPN) connection from the machine to anywhere via eWON's cloud-based remote connectivity solution, Talk2M (see Chapter 3). The router seamlessly communicates on the local area network (LAN) with the PLC and the HMI, using either an Ethernet four-port switch, a universal serial bus (USB) link, or a serial link (for legacy PLCs with serial ports). On the machine side, an eWON Cosy must to be installed and will be connected to a PLC, an industrial PC, or any automated device. Together, the solution allows remote connection with a PC, laptop, tablet, or smartphone.


TIP

eWON Cosy with Talk2M makes it easy to connect users to their machines via the Internet. Users don't need to be IT experts to take advantage of the solution (see Figure 4-1).

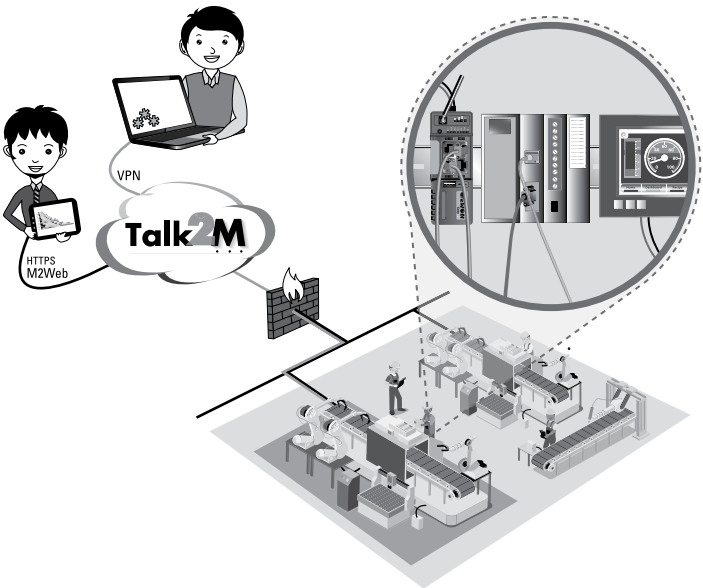

FIGURE 4-1: Talk2M provides cloud connectivity services to connect users to their machines via the Internet.

eWON offers users three ways to connect to their machines:

- Talk2M client software (eCatcher)
- Talk2M mobile app (eCatcher mobile)
- Talk2M web portal (M2Web)

On the user side, you simply install a client software application, called eCatcher, on a PC running Microsoft Windows. eCatcher establishes a VPN connection over the Internet between your PC and Talk2M.

The mobile version, eCatcher Mobile enables remote access from your favorite iOS or Android mobile device.


TIP

Alternatively, you can use a web browser (such as Google Chrome, Microsoft Internet Explorer/Edge, or Mozilla Firefox) without installing the eCatcher application, to connect to your machines (called M2Web), but this method is restricted to certain applications.

Connecting Your Machine to the Internet Using eWON Cosy

You have several options for connecting your machines to the Internet in order to communicate with the Talk2 server:

- **Local area network (LAN):** Most sites have a LAN that is connected to the Internet, so this is often the preferred method for connecting your machines to the Internet. An Ethernet LAN connection is typically cost-free and provides reliable, high-speed access. However, in some cases, LANs have complex security policies in place that may prevent your machines from connecting to the Talk2M server over the Internet. In these cases, Wi-Fi or cellular connections may be a better option.
- **Wireless network (Wi-Fi):** Wi-Fi networks are becoming increasingly common in many areas, including industrial plants and factories. Like LAN connections, Wi-Fi access is typically cost-free and provides high-speed connectivity.

Many sites provide "guest" Wi-Fi networks that are logically separated from the factory LAN, specifically to allow machine builders to get access to the Internet without requiring firewall configuration changes. Wi-Fi connectivity and coverage may be somewhat limited, particularly in noisy industrial areas that may interfere with Wi-Fi signals. In these cases, LAN or cellular connections may be a better option.

- **Cellular (2G, 3G, 4G):** When no LAN or Wi-Fi connection is available, cellular technologies may be a good alternative. Cellular service is typically available worldwide, albeit at different speeds (2G, 3G, or 4G), but signal coverage may be limited or unreliable in some remote areas. Also, data usage charges on a cellular network can be very high and cellular technology — for example, Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) — varies around the world, potentially requiring different Subscriber Identity Module (SIM) cards to be installed in the machine routers. LAN or Wi-Fi connections are typically preferred if they are available.

Connecting the Machine to Talk2M

Once connected to the Internet, the first thing the eWON does is to connect to the Talk2M servers.


TECHNICAL STUFF

The connection of a machine to Talk2M is performed in three phases (see Figure 4-2):

1. The eWON connects to a central access server (AS) and authenticates through a Hyper Text Transfer Protocol Secure (HTTPS) session.
2. The eWON requests the IP address of the VPN server it needs to use (VPN server addresses may change from connection to connection) via an HTTPS connection.
3. The eWON establishes a VPN tunnel with the VPN server.

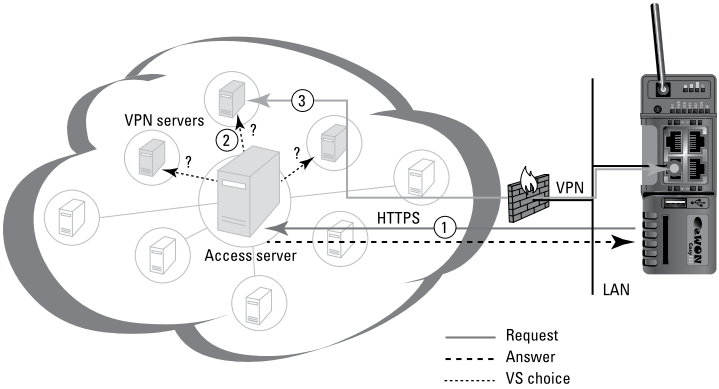

FIGURE 4-2: Connecting the eWON to Talk2M in three phases.

Connecting the User to Talk2M

When the user starts the eCatcher software on a PC, the first step is for the user to authenticate himself or herself using the following information:

- **Account name:** A Talk2M account can be created with eCatcher. An unlimited number of accounts can be created. Each account contains all the users who can connect to the eWON devices registered in that account.
- **Username:** An unlimited number of users can be registered in an account. Usernames within an account must be unique.
- **Password:** Each user has his or her own password. Do not use default passwords and do not share your password with anyone. Passwords should be at least 8 characters long — 12 or more characters is better — and should contain upper-case and lower-case letters, numbers, and special characters (such as !, #, $, or %) for better security.

WARNING

Treat your username and password like other sensitive personal information (such as your Social Security number or credit card information). The unique combination of a username and password, known only to you, establishes your identity on a system and associates you with any actions performed on a machine. If an attacker or any other unauthorized user performs malicious

actions on a machine using your username and password, you might be considered a suspect!

Once authenticated, you can access a list of all the eWON devices registered to an account. The eWON list provides:

- The name and status of the eWON device
- A brief description of the eWON device and machine
- Any users who are currently connected to the eWON device
- Any pools to which the eWON device is assigned. A pool is a collection of eWONs.
- The PLC type
- The remote access media type (such as LAN or cellular)
- The IP address of the camera (if installed)

When you click on any eWON device listed, if its connection status is marked "Online" (meaning a VPN connection is up and running), eCatcher creates a VPN tunnel to the assigned eWON device.

TIP

You can also perform several other actions in eCatcher, such as:

- Registering a new eWON device in the current account
- Modifying and deleting eWON device information
- Adding, modifying, or deleting user information or groups in the current account. A group is a collection of users.
- Adding, modifying or deleting pools in the current account
- Modifying the account information

Using the VPN Connection

When a VPN connection is established, two "tunnels" are created — one between the eWON and the VPN server, and another between the eCatcher and the VPN server (see Figure 4-3). Each tunnel is automatically assigned a unique VPN IP address. Although the VPN addresses are reachable from the eWON side and from the eCatcher side, they are not reachable on the VPN server side.

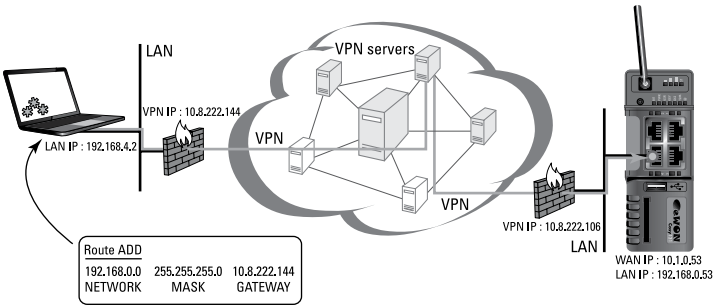

FIGURE 4-3: The eCatcher software automatically adds a route to the destination eWON's IP LAN address.

TECHNICAL STUFF

To reach the machine side of the eWON, your PC needs to know that all traffic containing a destination IP address in the eWON LAN IP address range should be forwarded through its virtual interface. To allow this, eCatcher automatically adds a route when a VPN connection is opened and automatically deletes the route when the VPN connection is closed (see Figure 4-3). The eCatcher software knows the eWON's LAN IP address because it is provided when each eWON registers itself in a Talk2M account. If you want to connect to another eWON, eCatcher automatically deletes the previous route and adds a new route with the appropriate destination address range.

On the machine side, the traffic coming through the VPN tunnel is forwarded to the LAN (machine) side of the eWON automatically. For a machine on the LAN side to communicate back to the PC, you have two options:

- A network address translation (NAT) feature (also called Plug'n Route) can substitute the eWON IP LAN address for the PC IP address (this is the default configuration in the eWON).
- Individual machines on the LAN side of the eWON can be manually configured to use the eWON's IP LAN address as its default gateway.

Getting to Know Other eWON Solutions

In addition to the eWON Cosy, eCatcher, and Talk2M remote access products, eWON offers many other industrial routers and devices including the eWON Flexy, eWON Netbiter industrial router with associated Argos cloud service, and the eWON eFive industrial VPN appliance.

Remote data with eWON Flexy

The eWON Flexy is a versatile Industrial Internet of Things (IIoT) gateway and remote access router designed for OEMs and system integrators. In addition to VPN remote access, it allows you to monitor and collect vital key performance indicators (KPIs) for analysis and predictive maintenance. It is also possible to integrate data into your own systems or cloud platforms using the Talk2M application programming interface (API).

Capabilities of the eWON Flexy include:

- **Extension cards:** On top of the basic functionality, it can be tailored to meet your specific connectivity needs by adding extension cards, now or when a future need arises. You can make it as simple or full-featured as you need it to be.
- **Secure VPN remote access:** The eWON Flexy embeds VPN capabilities and compatibility with Talk2M and eFive. This allows highly secure remote access for remote monitoring, troubleshooting, and application tuning. The Flexy 20x adds routing capabilities that allow remote access to any serial or Ethernet devices behind the eWON Flexy. It enables PLC remote maintenance, remote IP camera, remote HMI monitoring, and more.
- **Data acquisition:** Local data acquisition is performed by the eWON Flexy using the serial or Ethernet port. The data acquisition process is built around a tagged database in which each tag is associated with an input/output (I/O) server.
- **Alarm management and notification:** Full support for alarm triggering, acknowledgment, status, and traceability is provided by eWON Flexy. Alarm thresholds (for example, four times) and parameters (such as activation delay and deadband value) can be set on every tagname. The complete alarm cycle is traced and available for monitoring and

analysis. Alarm notification can be performed by email, Short Message Service (SMS) text, Simple Network Management Protocol (SNMP) trap, and/or File Transfer Protocol (FTP).

- **Data logging and retrieval:** Continuous data logging and buffering can be performed on every tagname. Each tagname can be logged on a fixed interval or change triggers (with deadband). eWON stores tag data values and timestamps in its internal database (up to one million timestamped points) for statistical analysis and later review (historical logging), or to analyze recent trends (real-time logging).
- **Web server HMI:** The eWON Flexy has an integrated web server for configuration and monitoring, viewable on any standard web browser.
- **Talk2M API:** Employ the API for enterprise integration of third-party software and cloud solutions (for example, eWON IIoT Partners, Amazon Web Services, GE Predix, IBM Bluemix, Microsoft Azure, and others).


TIP

Typical applications for the eWON Flexy include industrial machines, cleantech machines, photovoltaics, building management, smart metering, water and wastewater, energy monitoring, irrigation systems, energy meters, and others (see Figure 4-4).

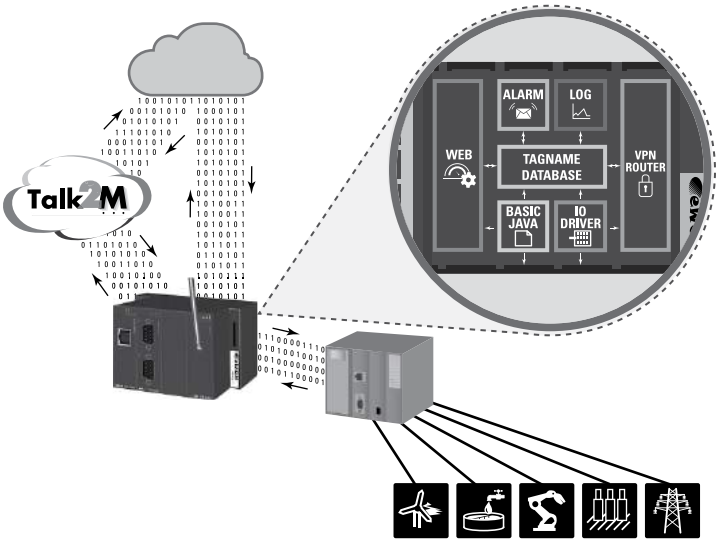

FIGURE 4-4: The eWON Flexy connects remote field equipment using different communication protocols.

TIP

For more information about the eWON Flexy, visit: `www.ewon.biz/flexy`.

Remote management with eWON Netbiter

With eWON Netbiter, the end-users/facility managers can stay on top of equipment status and operations remotely. You can track performance, receive alarms if something goes wrong, and remotely manage and configure their industrial assets via a PC or smartphone.

A Netbiter communication gateway connects to your equipment in the field. The gateway sends encrypted data via a wide area network (WAN) or mobile phone network to the Netbiter Argos data center in the cloud (see Figure 4-5).

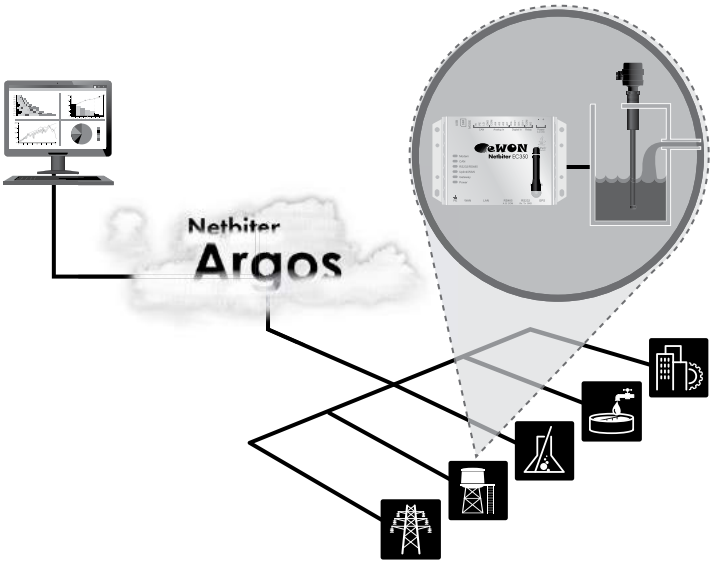

FIGURE 4-5: The eWON Netbiter and Argos cloud service.

The Netbiter Argos data center is a secure, cloud-based hosting service where all your data is stored and accessed. Netbiter Argos is packaged in two different services that meet different user requirements:

- **View and Control (one user — one site):** You can monitor and control equipment via online dashboards, trend graphs, and alarms for one user and one site. The View and Control service package is included with the purchase of your Netbiter gateway. Features include:
  - Monitor and control equipment remotely
  - Use dashboards, templates, and profiles
  - Manage alarms
  - View and download trend data
  - Google map view (including alarm)
  - Create and upload device templates
- **Manage and Analyze (multiple users — multiple sites):** You can manage multiple sites, equipment, and users. Manage and Analyze is a paid subscription service that includes all the View and Control service package features, as well as the following capabilities:
  - Access and manage multiple sites and installations
  - Manage and deploy profiles
  - Create and export data reports
  - Maintain a single access point to all systems
  - Manage users and projects

TIP

For more information about the eWON Netbiter and Argos, please visit: `www.ewon.biz/netbiter`.

Remote networks with eWON eFive

The eWON eFive allows system integrators to establish secure industrial networks. It employs permanent VPN connections to link multiple remote sites to central control rooms as well as to supervisory control and data acquisition (SCADA) systems. The eFive creates seamless access to your remote sites' data at any time (see Figure 4-6).

TIP

Typical applications for the eFive include water and wastewater, wind power generation, photovoltaics, biogas, and others.

To learn more about connecting SCADA to your remote sites, visit `www.ewon.biz/efive`.

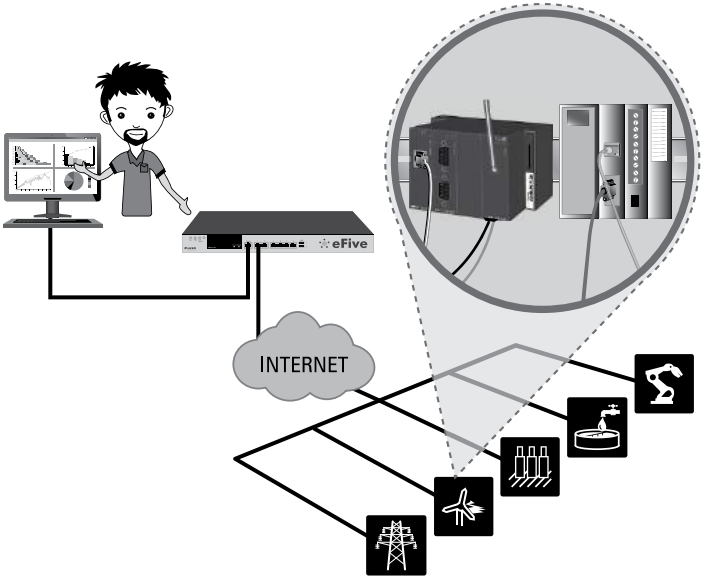

FIGURE 4-6: eFive securely connects your SCADA to your remote site PLCs.

IN THIS CHAPTER

- Sealing the deal for manufacturing
- Rising to the occasion for a large bakery company
- Putting the pedal to the metal for metal fabrication
- Improving and saving lives in the medical industry

Chapter 5
Exploring Remote Access Success Stories

In this chapter, four real-world eWON customers in different industries share their remote access success stories with you.

Manufacturing

Based in Chicago, MAAC specializes in manufacturing thermoforming machinery and other companion products. MAAC products are used around the world and serve many industry sectors, such as aerospace, medical, and automotive.

MAAC quickly learned that automation control technology is the key to success in the machinery sector. Leslie Adams, Director of Technical Services, has long been an advocate of electronic automation. According to Mr. Adams, "The communications provided by an eWON VPN router is simply incredible. Using an Internet connection, we can connect to machines just about anywhere. It eliminates the need for any kind of special interface."

The secure VPN connection that eWON technology provides offers full integration of IT security standards. eWON's unique

remote access solution allows MAAC to connect to machines in the field with the same ease and flexibility as a machine in the company's shop.

Remote access enables the company to connect to a machine just as if it were on-site, and to have access to Programmable Logic Controllers (PLCs), drives, and HMI devices, as well as any other device connected to the machine subnet, including an IP camera.

Before installing eWON routers, MAAC used phone modems to connect to its machines, though the delay time was a huge problem. "I remember the frustration associated with trying to monitor machines when it took a long time for information to make its way back via the modem connection. In one instance, we were working with a machine in Australia and the delay ran up to 15 seconds," recalls Adams.

Remote maintenance, which enables quick and efficient troubleshooting, has a positive impact on the customer's support costs. Leslie commented, "With eWON, we eliminate 50 to 70 percent of our support cost, in addition to significantly reducing hours of machine downtime normally associated with waiting for a service technician. Travel time wasted on field trips equates to a lot of money. Sitting in airports and driving out to customer installations means a whole lot of unproductive time. Time we prefer our programmers spend working on new machines or fine-tuning existing systems. When these guys are gone — they simply aren't working on the important stuff."

Food and Beverage

Bakkersland is the largest bakery company in the Netherlands. The main concern of Bakkersland is the possible standstill of machinery in a production process. Any standstill situation could lead to delays in the logistics process.

To avoid this kind of disruption, Bakkersland undertook a project in which each of its machines would be equipped with an eWON industrial router. The eWON routers are installed in the control room next to the PLC on the DIN rail (a metal rail used to mount circuit breakers and industrial control equipment inside equipment racks). The structure works online and can provide remote supervision of the machine to the operator through a secure VPN connection.

Bakkersland chose the eWON Cosy router as the remote maintenance system for its machinery. Vincent Wagenaar, Sales Director from Raster Products, the Dutch distributor for HMS, explains: "eWON has developed this product to meet the demand of a more simplified router with only basic features. Routers equipped with many features are often not used to their full potential. The eWON Cosy can be regarded as a replacement for the traditional modem, whereby the Cosy establishes an Internet connection immediately, rather than using a telephone connection."

Dennis van Scheijndel, from Bakkersland, explains the benefits of the eWON architecture: "If there is an alarm, the operator may be able to indicate that a particular sensor is dirty or that the connection isn't entirely secured. If necessary, the supplier will be able to make changes to the control. It is not only us as a user who wins in time; the machine manufacturer has no further need to send an engineer out. In particular, suppliers who are located abroad benefit from this."

Bulk Material Handling

A.G. Stacker is a manufacturer of state-of-the art stackers and ancillary equipment. When Clarence and Helen Allen launched the company in 1996, they had a goal to provide innovative equipment with better customer support than anyone in the industry. Today, keeping innovation and customer service in mind, A.G. Stacker is working with eWON to develop the next generation of customer interaction.

A.G. Stacker's machines have been adopted by customers around the globe. Each of these machines employs a sophisticated automation system including drives, programmable controls, and other state-of-the-art devices. While A.G. Stacker has a highly trained team of engineers, technicians, and trainers to assist customers in maximizing machine value, customer conditions sometimes warrant fine-tuning and system modifications in the field. Automation equipment on live machines sometimes requires someone to travel out to the customer to make even small changes. With the cost of last-minute flights skyrocketing, A.G. Stacker sought a new and innovative way to address the problem. This is where eWON was called in to help.

eWON provides a fast and easy, yet secure approach to remote connectivity. Kennedy Larramore, A.G. Stacker's electrical/IT technician

explains: "Even though we have three techs assigned to assisting our customers, "road techs" are costly for both our customers and A.G. Stacker. At the heart of the matter, time spent traveling can be better used by our people and downtime at our customers is very expensive. Further, we often encounter issues where the customer has a difficult time describing the exact nature of the problem."

"We started out providing the eWON devices as an option on our machines. But after witnessing the power of eWON's free Talk2M solution and the devices in the field, we have made eWON a part of every machine we build" says Kennedy.

Cyclotron Machines

IBA develops high-precision solutions for the diagnosis and treatment of cancer — for example, cyclotrons. IBA selected eWON and Talk2M technology to deliver remote service on a global scale.

"First and foremost, our goal is to be able to solve problems remotely for customers in the event of a failure or if there are questions," explained Patrick Delcour, IBA's Customer Service Project Manager. "With Talk2M, I can connect and switch from the Melbourne site in Australia to Ghent in Belgium in three seconds."

Faults are resolved for the customer from the control room based on the information provided by the status of indicator lights and the displays. "However, the information escalated from the control room is very fragmented," stressed Delcour. Before using eWON, when a problem occurred, the customer's operator had to call an IBA hotline.

The Talk2M solution has revolutionized IBA's way of working. Talk2M offers simplicity of use and connection while enhancing response efficiency. "Just three clicks and I'm connected," Delcour said. The complexity associated with firewalls or proxies is entirely hidden from the user.

Once the connection with Talk2M is established, all the IP addresses on the LAN side of the eWON become transparent and accessible to the user. In a few clicks, the user can connect to the PLC and the IP camera, or start the remote desktop application on the control PC to take over the local PC and launch the HMI.

Discover more eWON success stories at `www.ewon.biz/customers`.

IN THIS CHAPTER

- Creating and configuring your Talk2M account
- Configuring your eWON Cosy
- Connecting to your remote device

Chapter 6
Ten Easy Steps to Get Started with eWON Cosy 131

In this chapter, we walk you through getting started with the eWON Cosy 131 in these ten easy steps:


TIP

If you don't yet own an eWON Cosy, but are looking to get one, please visit `www.ewon.biz/contact` to find a distributor in your area/country.

1. **Download and install eCatcher.** eCatcher is a free companion tool used to initialize remote access across the Talk2M virtual private network (VPN) and connect to all devices plugged into your eWON. You can download eCatcher from the eWON website at `https://support.ewon.biz/software`. After launching the installation wizard, follow the instructions to complete the setup and launch eCatcher.
2. **Create your account by clicking Create a Free+ Account on the login page.** Create a unique account name, provide your name and email address, and create a password. You

also need to activate your account by clicking the link sent to your email address.


TIP

Click Check Availability to verify that you have selected a unique account name.

3. **Log in to eCatcher and add your eWON by clicking the Add button (see Figure 6-1).**

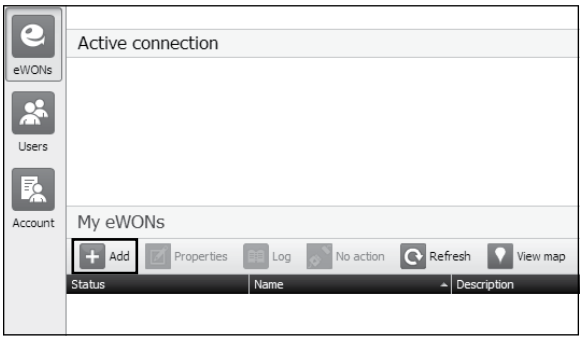

FIGURE 6-1: Adding an eWON in eCatcher.

Proceed by following the wizard. Copy the Activation Key to your clipboard (see Figure 6-2). This will be used for configuring the eWON in Step 8. Close the eCatcher application.

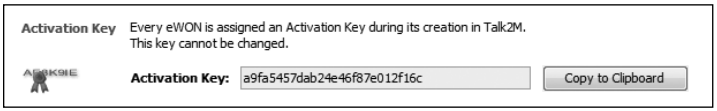

FIGURE 6-2: Copying the Activation Key to your clipboard.

4. **Download and install eBuddy.** eBuddy is eWON's free maintenance utility. It is used to read basic information about the eWON, set the network (IP) address, update the firmware, and back up or restore the system. You can download eBuddy from the eWON website at `https://support.ewon.biz/software`. After launching the installation wizard, follow the instructions to complete the setup and launch eBuddy.

5. **Connect an Ethernet cable from your computer to the eWON's local area network (LAN) port number 1 (see Figure 6-3).** Either a straight-through or crossover Ethernet cable will work.

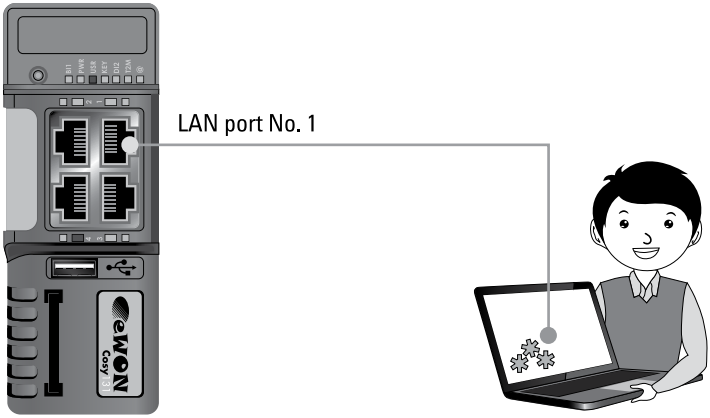

FIGURE 6-3: Connecting your computer to your eWON.

6. **Launch eBuddy and select Set IP Address to change the eWON's IP address.** Use an IP address that will not conflict with your network or any other remote computer's IP address. Set your computer's IP address to the same subnet as the eWON's IP address. You can learn more about setting the IP address here: `https://support.ewon.biz/set_lan_ip_address`.


TIP

Write down your computer's IP address information before changing it so you can return to its original state (and get back onto the Internet) after you're done.

7. **Launch your web browser and enter your eWON's IP address in the address bar.** Log in using the default username and password, which are both "adm".


WARNING

Change the default username and password immediately! Default usernames and passwords are *not secure* and are often used by attackers to breach systems and networks.

8. **Click on the Settings button and run the Quick Launch Wizard.** Configure the system, communication, and Talk2M connection settings. When prompted by the Talk2M connection wizard, paste the Activation Key you copied in Step 3.

9. **Plug the Internet cable into the wide area network (WAN) port.** The WAN port is number 4 (by default) on the bottom left of the eWON (see Figure 6-4). You can verify it by looking for the red LED light (instead of a green light) beneath the Ethernet port. When your settings are complete, unplug the Ethernet cable between the eWON and your computer and set the IP address of your computer back to its original state.

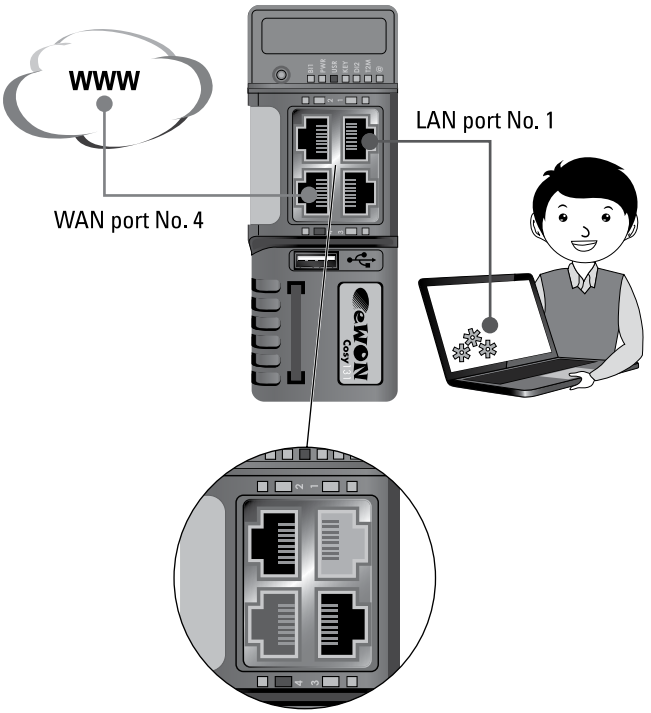

FIGURE 6-4: Identifying the WAN port on your eWON.

10. **With your computer connected to the Internet, launch eCatcher.** The status of your eWON should be Online. Simply highlight your eWON and click the Connect button.


TIP

After you're connected, if you have plugged an Ethernet device into your eWON COSY's LAN port, and in the same subnet, you should be able to ping its IP address to verify connectivity.

Glossary

2G: Commercially introduced in 1991 and based on GSM, the second generation of wireless telecommunications technology enabled digital data services for mobile, notably SMS text messages. *See also* Global System for Mobile Communications (GSM) and Short Message Service (SMS).

3G: Commercially introduced in 1998, the third generation of wireless telecommunications technology provides data transfer rates of 2 megabits per second (Mbps) or more for wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls, and mobile TV technologies.

4G: Commercially introduced in 2008, the fourth generation of wireless telecommunications technology provides peak data transfer rates of 100 Mbps for high-mobility communication (such as from a moving vehicle) and 1 gigabit per second (Gbps) for low-mobility communication (such as from a pedestrian).

Advanced Encryption Standard (AES): A symmetric block cipher algorithm that is used to encrypt sensitive network traffic and data. AES is the replacement encryption algorithm for DES and 3DES. *See also* Data Encryption Standard (DES).

asynchronous digital subscriber line (ADSL): A data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide. Commonly referred to simply as a digital subscriber line, or DSL.

application programming interface (API): A set of rules and specifications that software programs can follow to communicate with each other; serves as an interface between different software programs and facilitates their interaction.

certification authority (CA): An entity that issues digital certificates and certifies the ownership of a public key by the subject named on the certificate.

Code Division Multiple Access (CDMA): A channel access method used by various telecommunications technologies to enable multiple transmitters to simultaneously send traffic over a single communication channel.

Data Encryption Standard (DES): A symmetric key encryption algorithm developed in the early 1970s, but now considered insecure because of its small key size (56 bits).

DB9: A common electrical connector used for RS232 serial computer connections and named for its characteristic D-shaped metal shield and two parallel rows of nine total pins. *See also* RS232.

DF1: An asynchronous byte-oriented protocol used to communicate with most Allen Bradley RS232 interface modules. *See also* RS232.

Encapsulating Security Payload (ESP): Part of the IPsec protocol suite responsible for ensuring authenticity, integrity, and confidentiality of origin packets.

envelope encryption (EVP): A high-level interface for OpenSSL cryptographic functions. *See also* OpenSSL.

Ethernet: A network protocol that controls how data is transmitted over a LAN. Technically it is referred to as the *IEEE 802.3 protocol.* The protocol has evolved and improved over time and can now deliver data at the speed of 1GB per second.

Ethernet cable (crossover): A type of twisted pair copper wire cable with RJ45 connectors, used to directly connect two computing devices together.

Ethernet cable (straight-through): A type of twisted pair copper wire cable with RJ45 connectors, used to connect computing devices together on a LAN, typically via a hub or switch. *See also* local area network (LAN).

File Transfer Protocol (FTP): A standard network protocol used to transfer computer files between a client and server on a network.

firewall: A network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.

Global System for Mobile Communications (GSM): A wireless telecommunications standard developed by the European Telecommunications Standards Institute (ETSI) for 2G protocols. *See also* 2G.

human machine interface (HMI): The user interface in a manufacturing or process control system.

Hyper Text Transfer Protocol Secure (HTTPS): A protocol for secure communication via a web browser over the Internet that uses the Secure Sockets Layer (SSL) protocol for encryption. *See also* Secure Sockets Layer (SSL).

Internet Protocol (IP): The principal communications protocol in the TCP/IP communications suite for routing across network boundaries (routers) and the Internet. *See also* Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec): A network protocol suite that authenticates and encrypts data packets sent over a network.

Internet service provider (ISP): An organization that provides its customers with access to the Internet.

intrusion detection system (IDS): A hardware device or software application that monitors a network or system for malicious activity.

IP camera: A video camera that is networked over a Fast Ethernet connection. The IP camera sends its signals to the main server or computer screen via an Internet or network link. It is mostly used in IP surveillance, closed-circuit television (CCTV), and digital videography. IP cameras are widely replacing analog cameras because of their digital zoom and remote surveillance options over the Internet.

keyed-hash message authentication code (HMAC): A message authentication code that uses a cryptographic hash function and a secret cryptographic key.

local area network (LAN): A computer network that connects computers and devices (including machines) in a building, factory, lab, school, or other relatively limited area.

machine-to-machine (M2M): Wired or wireless communication that occurs directly between two devices.

Modbus: A serial communications protocol originally published by Modicon (now Schneider Electric) for use in its PLCs. *See also* programmable logic controller (PLC).

multi-factor authentication (MFA): A type of access control that only grants access after at least two forms of authentication are provided.

network address translation (NAT): A method for mapping an IP address to a different IP address, such as a private IP address to a public IP address.

network latency: Any kind of delay that happens in data communication over a network. Network connections in which small delays occur are called *low-latency networks.* Network connections that suffer from long delays are called *high-latency networks.*

network segregation: Separating one network into two LANs, keeping the unsafe computers in the front network and moving the computers that you would like to protect to a second, shielded network.

Object Linking and Embedding (OLE): A proprietary Microsoft technology that allows documents to be embedded and linked to other objects.

OpenSSL: An open source implementation of the SSL and TLS protocols. *See also* Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

original equipment manufacturer (OEM): A company that produces parts and equipment that may be marketed by another manufacturer.

out-of-band management: A dedicated communications channel used for management networked devices, such as monitoring and remote configuration. An out-of-band communications channel is independent of an in-band communications channel and is therefore not reliant on the device's operational communications channel (for example, a network connection).

packet switching: A method used in communications networks in which data is transmitted as packets — consisting of a header and payload — to its destination. Using information in the header, networking hardware routes individual packets to the destination over the best available path, then re-assembles the data in the correct order at the destination.

plain old telephone service (POTS): A basic analog telephone service.

Process Field Bus (PROFIBUS): A standard for fieldbus communication in automation technology.

programmable logic controller (PLC): A ruggedized industrial computer that has been adapted for the control of manufacturing processes.

public key infrastructure (PKI): A set of roles, policies, and procedures used to create, manage, distribute, use, store, and revoke digital certificates and manage public key (also known as *asymmetric*) encryption.

public switched telephone network (PSTN): The aggregate of the world's circuit-switched telephone networks operated by national, regional, and local telephony operators.

role-based access control (RBAC): A method of controlling access to computer or network resources based on defined roles assigned to individual users within an organization.

RJ45: A standardized telecommunications network interface ("registered jack") used for connecting voice and data equipment.

RS232: A telecommunications standard for serial transmission of data.

RS485: A standard serial interface defined by the Telecommunications Industry Association and Electronic Industries Alliance (EIA/TIA). Also known as TIA485 and EIA485.

Secure Hash Algorithm (SHA): A family of cryptographic hash functions published by the U.S. National Institute of Standards and Technology (NIST).

Secure Sockets Layer (SSL): A cryptographic protocol for secure communications over a computer network.

service-level agreement (SLA): An official commitment between a service provider and a client that addresses specific aspects of the service provided such as quality, performance, availability, and responsibilities.

Short Message Service (SMS): A text messaging service.

Siemens Multi-Point Interface (MPI): A proprietary serial interface based on the EIA485 (formerly RS485) standard used to connect PCs, consoles, and other devices to Siemens SIMATIC S7 programmable logic controllers. *See also* RS485 and programmable logic controller (PLC).

Simple Network Management Protocol (SNMP): A standard Internet protocol used to collect and organize information about managed devices on a network.

Subscriber Identity Module (SIM): An integrated circuit (IC) that is used to store the international mobile subscriber identity (IMSI) number and its related key, used to identify and authenticate subscribers on mobile devices.

supervisory control and data acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces (GUIs) for high-level process supervisory management.

ping: A software utility used to test the reachability of a host (such as a device or machine on an IP network).

Transmission Control Protocol (TCP): One of the core protocols of the Internet Protocol suite, TCP is one of the two original components of the suite, complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration, and file transfer rely on. *See also* Internet Protocol (IP).

Transport Layer Security (TLS): A cryptographic protocol for secure communications over a computer network.

Universal Serial Bus (USB): An industry standard that defines cables, connectors, and communications protocols for connection, communication, and power supply between computers and devices.

Virtual Network Computing (VNC): A graphical desktop sharing system used to remotely connect to and control another PC by sending keyboard strokes and mouse movements to a remote PC.

virtual private network (VPN): A technology used to securely extend a private network (such as a LAN) across a public network (such as the Internet) using an encrypted connection and data encapsulation. *See also* local area network (LAN).

wide area network (WAN): A telecommunications or computer network that extends over a large geographical distance.

wireless modem: A modem that bypasses the telephone system and connects directly to a wireless network, through which it can directly access the Internet connectivity provided by an Internet service provider (ISP).

X.509: A cryptographic standard that defines the format of public key certificates.

eWON

HMS

Stop traveling on site for support. Let's stay Cosy!

eWON **Cosy**

Easy VPN Remote Access to PLCs, HMIs, etc.

- Firewall friendly solution
- Proven solution counting Millions of VPN connections
- Free VPN service
- Compatible with major PLC brands

control design
FOR MACHINE BUILDERS
Readers' choice awards
#1 choice
in Remote Access

www.ewon.biz

Keep your machines humming — remotely

After-sales service and support for industrial machines is costly and time consuming. Experienced engineers and technicians travel to customer sites to diagnose issues, answer questions, provide training, and resolve problems. Wouldn't it be awesome — for you and your customers — if you could quickly and securely perform diagnostics and resolve most of those issues remotely? This book shows you how.

Inside...

- Learn how remote access has evolved
- Protect your machines from cyberattacks
- Connect to virtual private networks
- Discover real-world success stories
- Explore helpful remote access tools
- Get started with easy setup steps

Jon Jacobsen is Marketing Manager for the eWON Business Unit at HMS Industrial Networks. **Lawrence Miller** is the author of more than 60 For Dummies books.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-41339-4
Part number: MKTGA0030_EN
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.