White Paper

Secure Distributed Industrial Networks

Service-aware switches are the basis for an optimized network

RAD data communications
The Access Company

Contents

1 Introduction

The proliferation of Industrial Ethernet as the main infrastructure for mission-critical processes is raising concern about the vulnerability of these networks to cyber security threats.

The Stuxnet virus, initially reported in July 2010, was the first known malware specifically designed to damage industrial automation equipment. Computers with Siemens Step7 industrial control systems (ICS) were infected with Stuxnet via USB memory devices and the network. The malware targeted Simatic programmable logic controllers (PLC) to modify their software in a way that, over time, discretely damaged overall production-line operation.

Stuxnet raised awareness of cyber attacks on an ICS but similar attacks already occurred years before.

A famous case involved Maroochy Shire Council's sewerage system in Australia in 2000. A dissatisfied sub-contractor engineer remotely accessed the Maroochy Sewerage SCADA System with radio equipment and modified the operation of the sewerage pumping stations. The sub-contractor accessed the system multiple times over three months, causing 800,000 liters of raw sewage to spill out into local parks and rivers.

Another area of concern is national infrastructure like the electricity grid. According to a 2009 report in The Wall Street Journal, U.S. intelligence officials stated that cyber-spies repeatedly gained access to the national electricity grid and left behind software programs that can later be used to disrupt the system. Furthermore, an experiment in 2007 showed that hacking into a replica of a power plant control system caused the generator to self-destruct due to the changes made in its operating cycle.

The risk for cyber attacks on an ICS has significantly increased with the growing use of industrial networks. The migration of the ICS from proprietary local connectivity to an open standard network introduces new security vulnerabilities. Additional factors specific for industrial applications intensify the security risk:

- Use of highly automated systems that are often deployed in unmanned facilities and over a wide geographic area. Penetration to a remote part of the network and activation of malware that discretely damages the operation over time is a highly feasible scenario.
- Lack of security tools on the industrial end-devices (due to the tendency to avoid software updates, lack of processing power to add security mechanisms and lack of awareness). As a

result, temporary penetration to the internal industrial network is sufficient for attacking the industrial end-devices and generating long-term damage.

- Critical applications in which damage is not only measured by its impact on business but also on critical national resources and on civilians and the environment is extremely acute.

In view of the above, it's clear that any modern industrial automation network that uses Ethernet-based infrastructure needs to implement proper security measures. Due to the unique characteristics of industrial applications, existing security concepts from the enterprise world do not necessarily apply; and new security concepts for industrial control systems need to be defined and implemented.

2 Common Security Model

The typical security concept for industrial networks is based on a private network that is not connected to the Enterprise network or the Internet. Connection of the industrial devices to this private network is controlled based on physical authentication, so that only MAC or IP addresses specific per network port can be connected.

Such a network security concept is vulnerable in several scenarios:

- When a private network is connected over unsecured links like inter-connecting private sites using a public transport network. A hostile device that gains access to such an unsecured link can monitor the traffic of the private network, potentially modify it or deduce critical application information that can be later used to penetrate the network.

- When an external entity obtains temporary access to a private network, as is the case of technicians connected either locally over their laptop or at a remote service center. Temporary access can be used to infect the valid network entities with malware that will later damage the network.

- When an attacker gains physical access to some devices in a secure network (e.g., the physical penetration of an unmanned remote site of a utility with a significant number of sites). In this case the attacker can use local storage devices (i.e., a USB memory stick) or local communication interfaces (i.e., a serial console) to infect the valid network entity with malware that will later damage the network. In addition, the attacker may use such physical access to connect a hostile device with legal physical characteristics to a network port (i.e., modifying MAC address to fit the network rules) and gain access to the network.

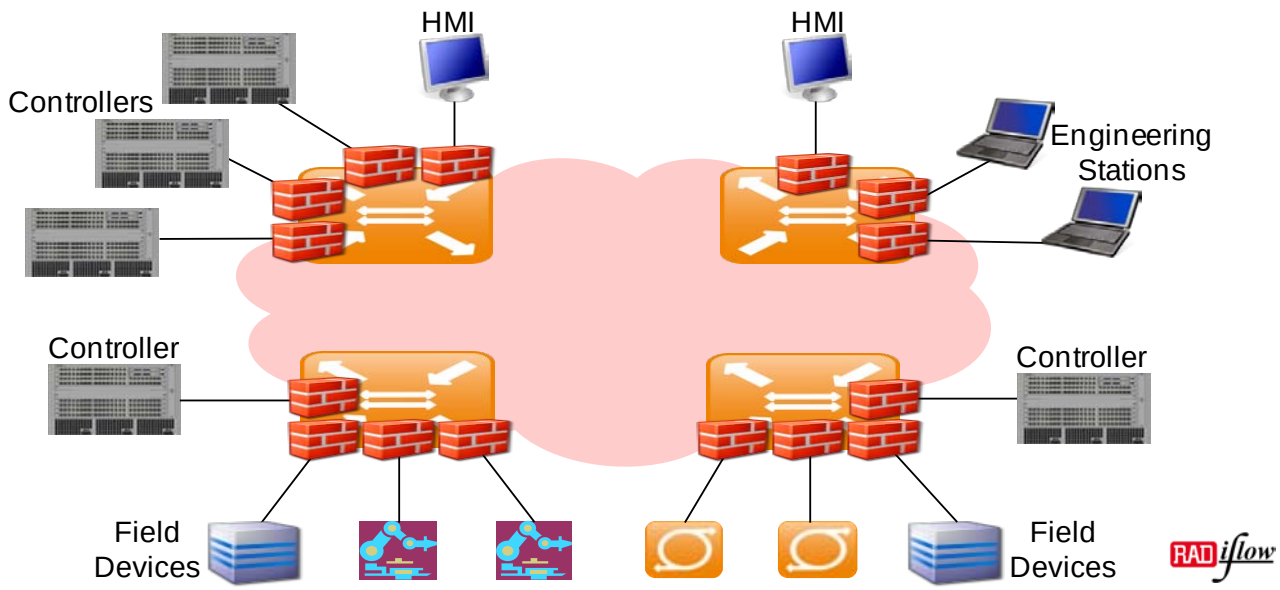
3 Distributed Service-Aware Security

Defending all the potential penetration points mentioned above is mandatory, but not sufficient. In view of the critical nature of industrial applications, an additional layer of security should be deployed to protect the industrial devices from an insider attack, in case a hostile entity gains access to the private network.

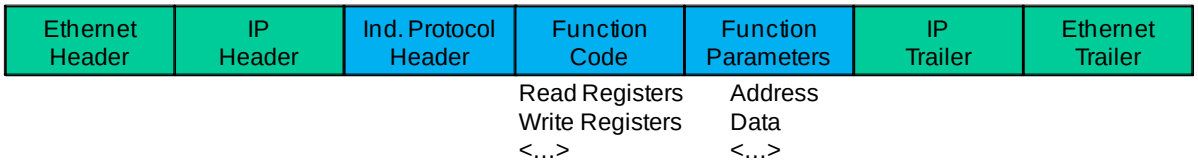
The best solution would be a personal firewall installed in each end-device that verifies that communication to and from the device conforms to the application logic defined by the network operator. This, however, is unlikely to materialize in the coming years due to the conservative evolution of industrial devices. An equivalent alternative is to deploy a service-aware firewall on the communication link between each end-device and the network. Such a firewall should understand the industrial automation protocol being used by the application, so it can monitor the detailed communication flow and verify it according to the application logic.

The resulting distributed service-aware security deployment will monitor all traffic at the edges of the network and verify that the communication of application-level commands and responses between all devices follows the valid application logic, as defined by the network operator.

RADiFlow's service-aware Industrial Ethernet switches offer a unique patent-pending solution for such a distributed deployment in industrial networks. RADiFlow switches contain a powerful co-processor for processing industrial protocols with an optimized internal link to the system switching matrix, so that selected traffic can be re-directed to the industrial co-processor for further processing. Using its built-in protocol processing capabilities, RADiFlow switches offer an integrated service-aware firewall, deployed next to each end-device as part of the network infrastructure. This eliminates the need to add a stand-alone firewall appliance at each port.



The service-aware firewall currently supports the Modbus and IEC60870-5-104, and will soon be enhanced with support for additional protocols such as IEC61850, DNP3, ProfiNet, OPC, etc. Based on its flexible processing engine, support for additional protocols can be added if their structure is well-defined.



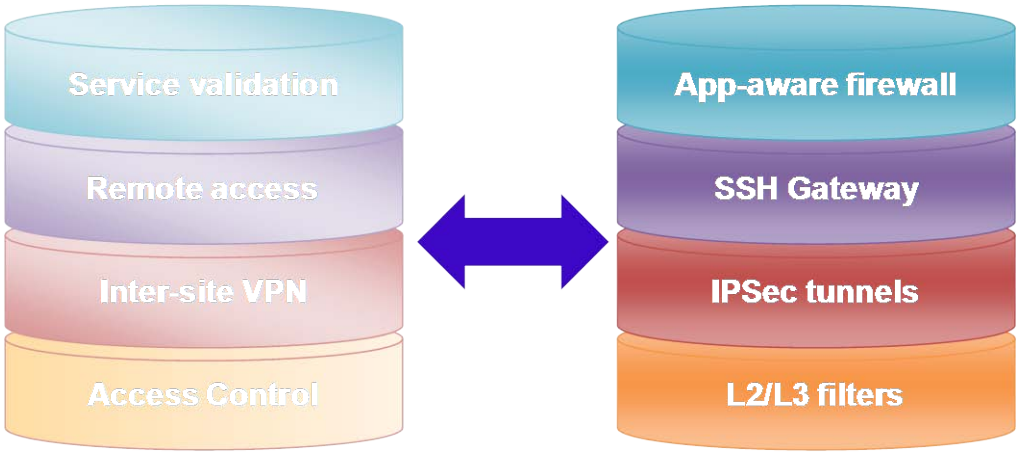
The service-aware firewall checks each packet's details, including:

- Protocol validity – that the packet structure and all its control fields comply with the standard and that the session flow follows the expected logic (i.e., session initiated by master, response matches request, session setup sequence, etc.).
- Application logic – verifies that only the allowed communication is performed between each pair of source and destination devices, by checking the function code and the command parameters according to operator-defined values.
- Abnormal patterns – monitoring communication per device in search of abnormal application behavior, such as repetitive use of specific sensitive commands (reset, clear history, etc.), burst of traffic beyond a reasonable threshold, etc.

The distributed service-aware firewalls in the switches are complemented with a service management tool that enables the network-wide configuration of valid application logic by the operator, logic that is then translated to specific firewall rules for each switch.

4 RADiFlow Defense-in-Depth Tool Set

In addition to the service-aware firewall, RADiFlow switches provide integrated support for a comprehensive set of security tools, so that a complete defense-in-depth solution can be deployed in the network without adding dedicated security appliances on top of the Industrial Ethernet infrastructure.



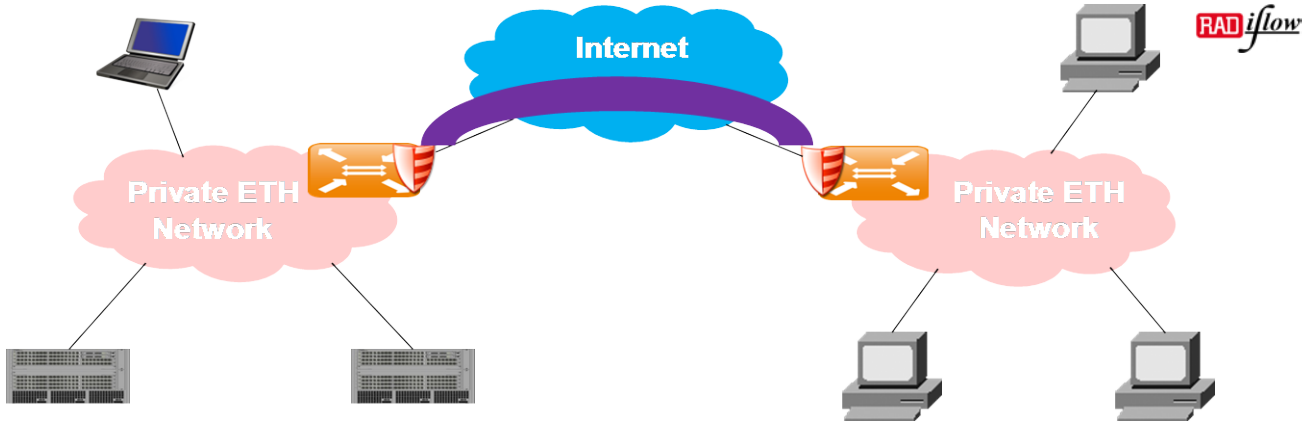
4.1 Network Access Control

The basic level of security for industrial devices connecting to the network is based on physical authentication. Each device attempting to connect needs to be authorized, per RADiFlow port, according to its MAC or IP address. This is achieved in one of two ways:

- The configuration of ACL (Access List) rules per port, to allow only devices with specific MAC or IP addresses to be connected to this port.
- User authentication using IEEE 802.1x protocol, in which the switch passes the authentication request from the end-device to a central RADIUS server to verify its access rights before opening it up to regular traffic.

4.2 Inter-Site VPN

In some cases, a distributed operational network has to use public transport links to connect between the sites. For example, in the case of a nationwide utility, some sites may have private fiber connectivity while some remote sites may need to be connected over leased virtual links (using 3G, DSL, etc.). When inter-site connectivity uses such a public infrastructure, the traffic must be encrypted to ensure its confidentiality and integrity.



Such a VPN (Virtual Private Network) connection is supported by the RADiFlow switches using GRE tunnels over an IPSec encrypted link. The use of IPSec encryption ensures the privacy of the link that is being transported over a public network. The IPSec tunnel can use 3DES or AES encryption according to the user configuration. The use of GRE tunneling, which supports Ethernet traffic, enables transparent connection of the sites as a single Ethernet network without having to set up IP routing logic between them. So, for example, when the network uses VLANs to identify the services, the GRE tunnel will preserve the VLAN information while a regular IPSec tunnel strips the VLAN information and passes on only the IP data.

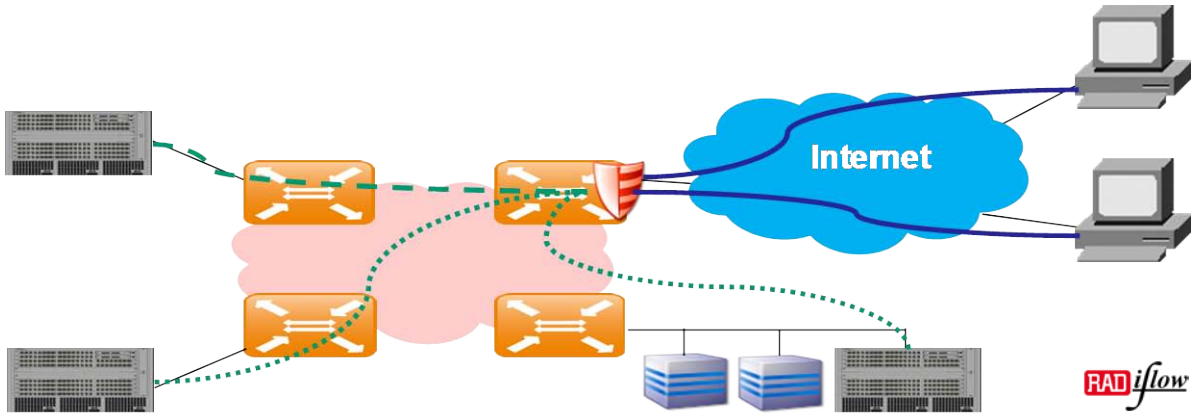
4.3 Secure Remote Access

When a remote user needs to access a secure network for operational or maintenance tasks, it's critical to ensure that only the limited set of authorized activities are enabled and are performed in a strictly secure manner. When remote access is initiated by an individual from an unknown location, a VPN connection as described above is too vulnerable. Instead, a more controlled tunnel with limited access rights should be used.

The RADiFlow switches feature an integrated SSH server to enable such limited remote access for operation and maintenance. Located at a secure site but connected to the outside world, the SSH

server enables remote users, such as field technicians, to log in over an encrypted communication channel. To enhance security, the server can restrict a technician's remote access so that it will be authorized only if the SSH server itself initiates the session. After the SSH tunnel is created, the access is controlled per user log-in authentication and specific access authorizations that are configured either locally in the switch or retrieved from a central RADIUS server.

Originally, SSH was planned as a secure terminal, but it's now used as a secure transport for any IP-based session. As a result, the SSH gateway is used for secure remote access for any protocol by simply re-routing the traffic in the remote computer to a local host, then encapsulating it over the secure SSH tunnel to the secure network. In this setup, the switch acts as a session proxy, so that the local network structure at the secure site is not exposed externally and further on-line security checks are performed in a manner similar to the functionality of the service-aware firewall.



4.4 Application-Aware Firewall

As noted above, RADiFlow switches contain an integrated firewall on each port, providing a distributed, network-based security solution that is equivalent to the use of personal firewalls on all the industrial systems in the factory.

Such a distributed deployment of service-aware firewalls is used to validate the application logic as it's represented in the communication flow between all devices in the network.

5 RADiFlow Portfolio

The RADiFlow family of service-aware Industrial Switches includes a comprehensive Ethernet and IP feature-set and is specifically designed for the harsh conditions of an industrial environment. The portfolio ranges from a compact 2 x GbE+8 x 100 switch for remote locations to a modular 28 x GbE switch for central locations.

The switches also have multi-service capabilities supporting various interface modules:

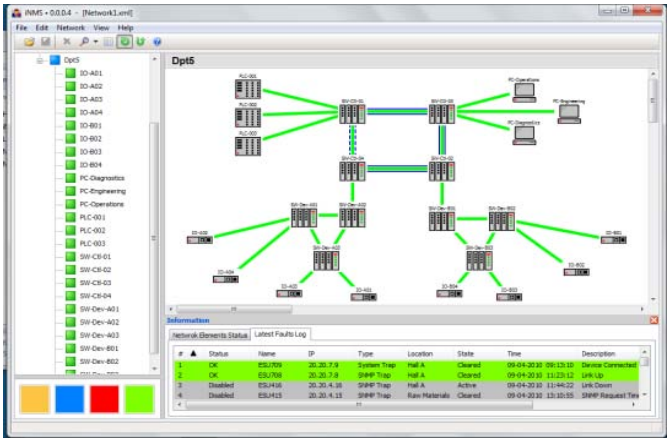
- Ethernet 10/100/1000 copper and 100/1000 fiber. The fiber interfaces are provided using SFPs for maximal flexibility.
- Serial RS-232/RS-485 used for connectivity of legacy devices to an Ethernet network. The switch can provide tunneling services to connect remote serial links or gateway services to translate the industrial automation protocol from its serial variant to the equivalent packet variant.
- Integrated modems for selected transport media (3G, DSL) to carry the Ethernet data-stream over various transport media.

These integrated multi-service capabilities enable network setup that fits a wide variety of real-life topologies using a single platform of network devices, thereby yielding a simple and cost-effective solution.

The iSIM service management tool supports the operation and maintenance of the network and services and requires minimal IT knowledge. The main features of the iSIM are:

- Management of the network topology, including RADiFlow switches and the industrial end-devices, including auto-discovery, topology management and network diagnostics.

- Service provisioning of end-devices' connectivity at the application level and of the security access rules between end-device pairs. The connectivity and security rules of the service group are automatically translated to configuration rules for the Ethernet switches and the embedded firewalls.

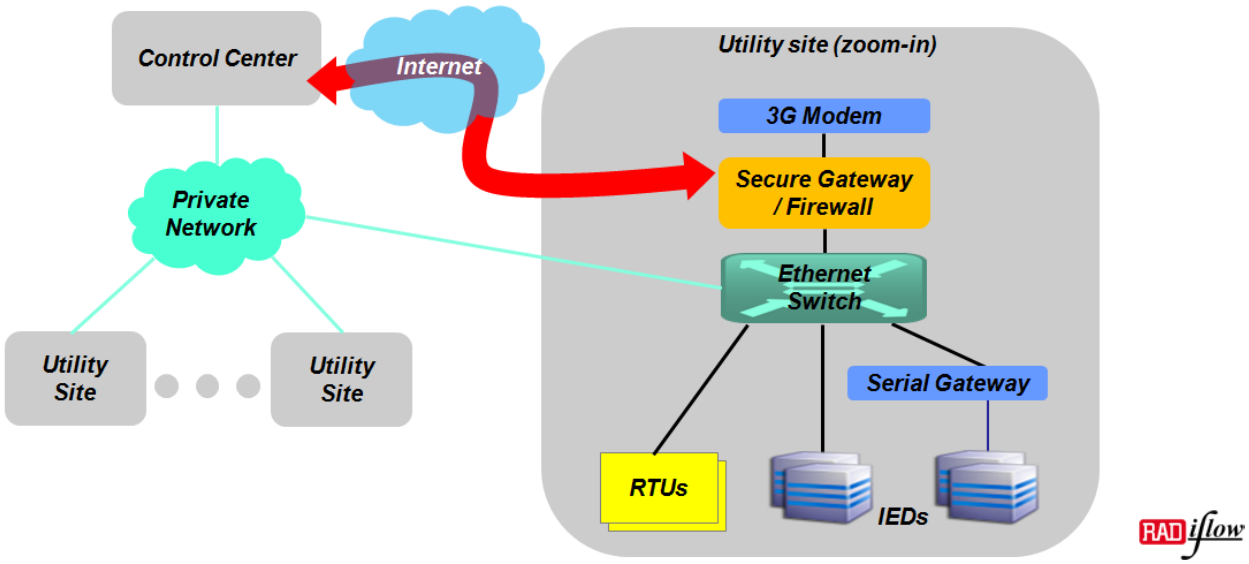


6 Reference Cases

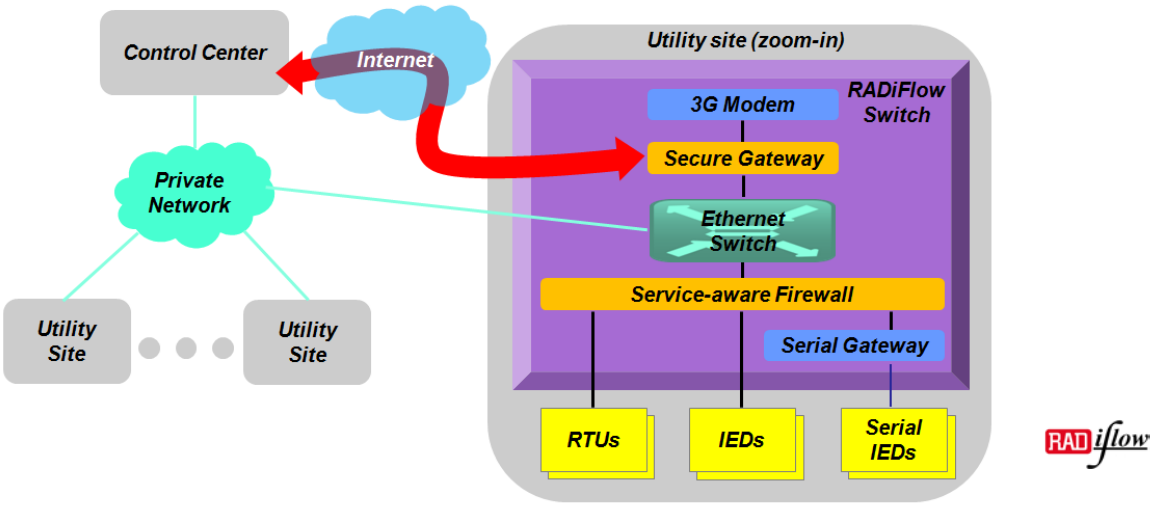
RADiFlow service-aware Industrial Ethernet switches provide an extensive feature-set to enable deployment of a simple and secure network for a wide variety of application topologies.

6.1 Distributed Utility

A nationwide utility has many distributed sites that need to be inter-connected. Such a typical site would include an Ethernet switch, serial gateways to connect the legacy devices and an optional 3G cellular modem for a remote site outside the reach of the utility private network. Furthermore, as discussed above, an application-aware firewall should monitor all the traffic to the devices and a secure VPN gateway should encrypt the data flowing over the public cellular network in order to provide a proper security solution.

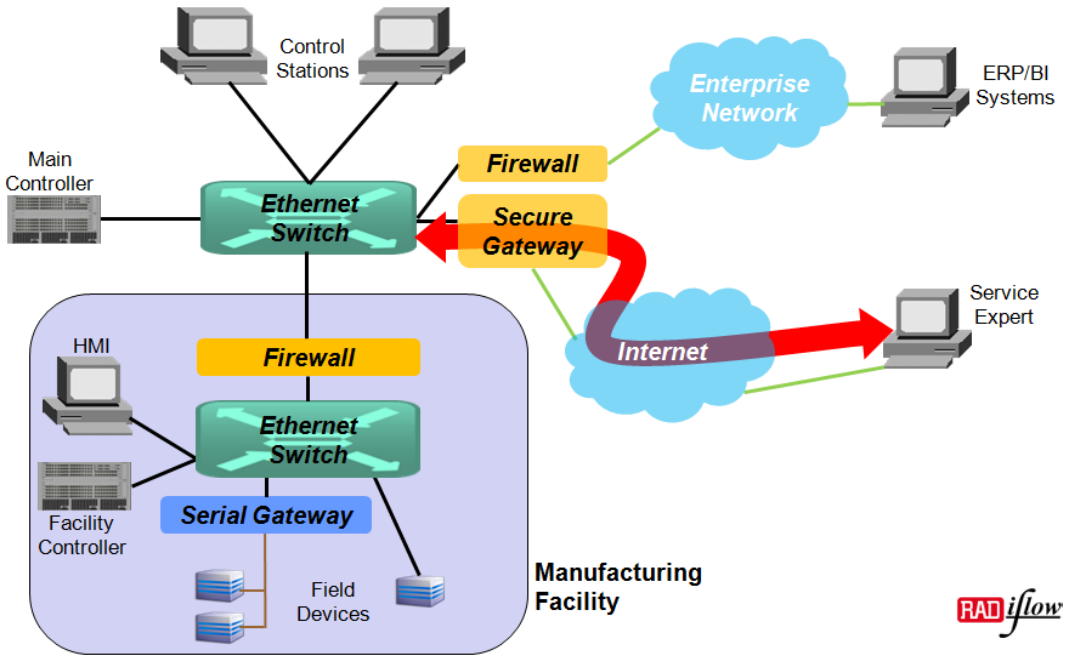


Using the RADiFlow service-aware switch, this site can be greatly simplified using its integrated functions, including its serial gateway, service-aware firewall, IPSec VPN gateway, and a 3G modem.

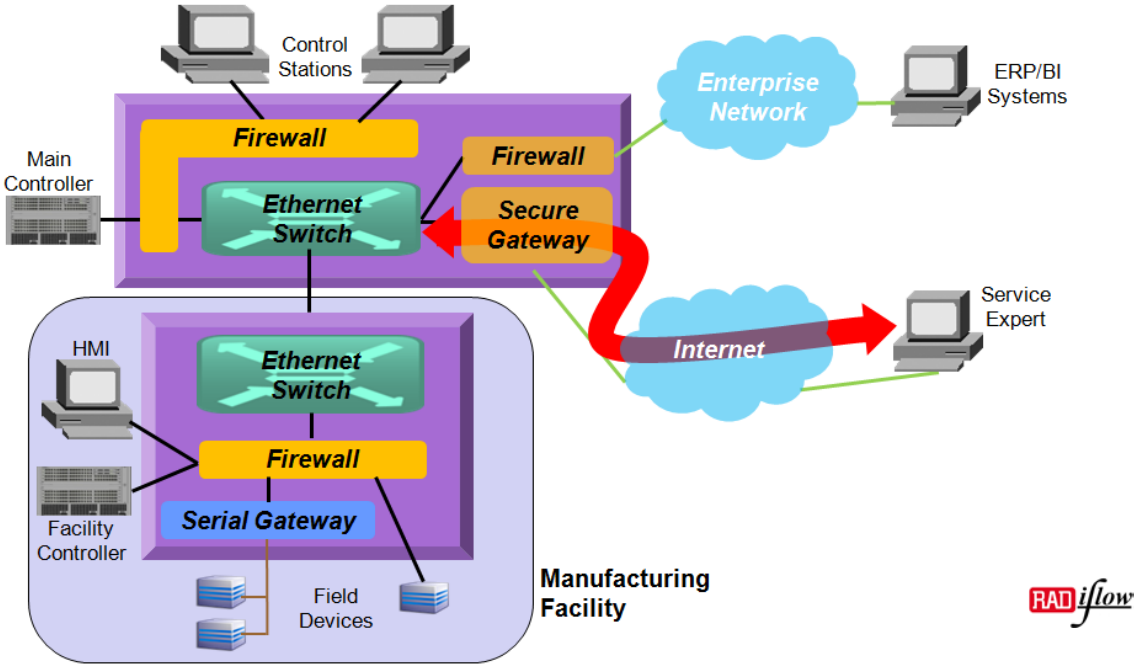


6.2 Modern Factory

A modern factory uses Ethernet throughout its production process, from the control to the device level. External connections to the enterprise network and remote operators or to service experts are required and should be properly secured. Such a typical factory would include an Ethernet network, serial gateways to connect legacy devices, firewalls between the zones, and a secure gateway for remote access over the Internet.



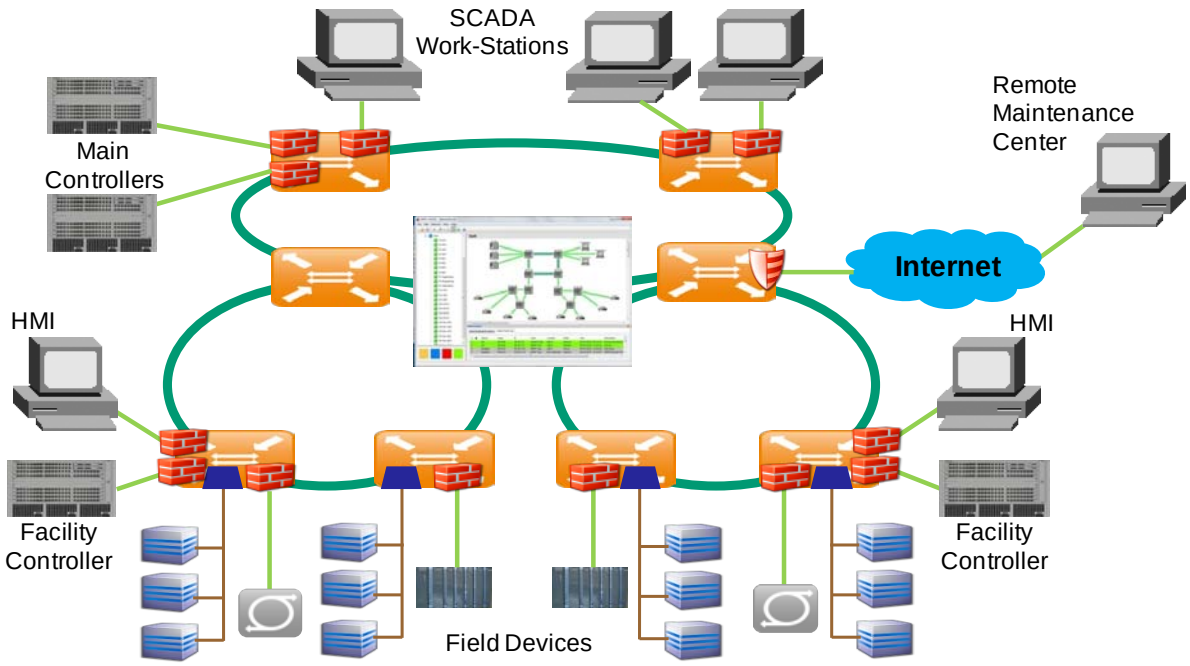
Using the RADiFlow service-aware switch, this factory can become more secure using distributed firewall deployment while still maintaining simplicity by taking advantage of the switch's integrated functions, including the serial gateway, service-aware firewall and SSH gateway.



7 Conclusion: Why RADiFlow?

The increased usage of Industrial Ethernet networks has raised concern about cyber security threats that can damage mission-critical industrial applications. As a result, there is a clear need for a comprehensive defense-in-depth solution dedicated to industrial networks, while keeping the overall network design simple.

RADiFlow provides a unique solution with an application-aware firewall engine integrated into its Industrial-Ethernet switches. This combination serves as the basis for easy deployment of strict



security measures throughout the internal communications network. Moreover, the RADiFlow portfolio is comprised of various size switches with a modular multi-service architecture that supports legacy serial-based and Ethernet devices. This enables network evolution and supports the growing need for Ethernet ports and bandwidth. The complete RADiFlow solution is complemented by the iSIM service management tool to support easy operation and network maintenance.

For more information about RADiFlow products: www.rad.com

www.rad.com

International Headquarters
RAD Data Communications Ltd.
24 Raoul Wallenberg St.
Tel Aviv 69719 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com
www.rad.com

North America Headquarters
RAD Data Communications Inc.
900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100,
Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com
www.radusa.com

RAD
data communications
The Access Company

Catalog no. 802500 Version 11/2011