Securing Power Generation with Unidirectional Security Gateways

A Unidirectional Reference Architecture

August 2015
Copyright © 2015 by Waterfall Security Solutions Ltd.
All Rights Reserved.
- Legal Notice & Disclaimer -

Any and all third party intangible and/or proprietary and/or intellectual property rights ("Third Parties’ Rights"), mentioned herein, whether registered or not, including, without limitation, patents, trademarks, service marks, trade names, copyrights and computer applications, belong to their respective owners. Waterfall Security Solutions Ltd. disclaims any and all interest in all such Third Parties’ Rights. It is forbidden to copy, modify, amend, delete, augment, publish, transmit, create derivative works of, create or sell products derived from, display or post, or in any other way exploit or use such Third Parties’ Rights without the express authorization of their respective owners.

Except as specified herein, Waterfall Security Solutions Ltd. does not guarantee nor make any representations with regard to any and all third party tangible and/or intangible and/or proprietary and/or intellectual property ("Third Party Property") mentioned herein. Waterfall Security Solutions Ltd. does not endorse nor makes warranties as to the completeness, accuracy or reliability of such Third Party Property, and all such warranties are hereby expressly and strictly disclaimed.
- Table of Contents –

EXECUTIVE SUMMARY .............................................................................................................. 4
MODERN THREATS .................................................................................................................... 5
IT-CENTRIC SECURITY NOT ENOUGH FOR POWER PLANTS .............................................. 6
MODERN PROTECTIONS: UNIDIRECTIONAL GATEWAYS ................................................... 7
USE CASE: SAFE IT/OT INTEGRATION .................................................................................. 8
  HISTORIAN AND DATABASE REPLICATION ........................................................................ 8
  OPTIONAL: SECURITY UPDATES ....................................................................................... 8
  OPTIONAL: SIEM AND OTHER IT INTEGRATIONS .......................................................... 8
  SECURITY BENEFITS ........................................................................................................ 9
USE CASE: VENDOR REMOTE MONITORING ........................................................................ 10
  VENDOR MONITORING .................................................................................................... 10
  OPTIONAL: REMOTE ADJUSTMENT .................................................................................. 10
  SECURITY BENEFITS ........................................................................................................ 10
USE CASE: CONTROL CENTER COMMUNICATIONS ............................................................ 12
  SECURE CONTROL OF PEAKING PLANTS ....................................................................... 12
  SECURITY BENEFITS ........................................................................................................ 12
USE CASE: PROTECTING RELAY AND SAFETY NETWORKS ............................................... 13
  SECURE MONITORING OF SAFETY AND PROTECTION SYSTEMS ................................ 13
  SECURITY BENEFITS ........................................................................................................ 13
NERC CIP COMPLIANCE BENEFITS .................................................................................... 14
  EXEMPTIONS FROM 30% OF NERC CIP V5 REQUIREMENTS ........................................ 14
  NERC CIP V6 ..................................................................................................................... 15
COST SAVINGS ........................................................................................................................ 16
  IT/OT COST SAVINGS ..................................................................................................... 16
  OTHER COST SAVINGS ................................................................................................. 16
  THE COST OF RISK ........................................................................................................ 17
UNIDIRECTIONAL REFERENCE ARCHITECTURE ................................................................ 18
WHICH OF OUR CONTROL SYSTEMS IS EXPENDABLE? ....................................................... 20
ABOUT WATERFALL SECURITY SOLUTIONS .................................................................... 21
Executive Summary

Cyber threats become more sophisticated over time, and so our defenses must continue to evolve as well. Traditional IT-style defensive architectures depend unduly on firewalls and intrusion detection systems. Firewalls allow attacks to pass from untrusted to trusted networks. Intrusion detection systems detect some attacks, and miss others. In most cases detecting, investigating and remediating intrusions takes so long that intrusion detection systems are not effective at preventing attackers from achieving their cyber-espionage, cyber-sabotage or equipment-damaging goals. This is unacceptable.

This paper describes a modern reference architecture for defense-in-depth network protection of power plants, illustrated in Figure (1). The architecture recognizes that every computer, device or machine exchanging messages with the Internet is potentially compromised and therefore untrustworthy, and that every machine exchanging messages with an untrustworthy machine is similarly untrustworthy. In the Figure then, only the green and blue plant networks are trustworthy. These networks are protected by Unidirectional Gateway technologies, whose stronger-than-firewalls protections eliminate the threat of network attacks from untrusted networks, and eliminate external network-connectivity cyber risks to protected, reliability-critical networks.

This architecture supports all business needs and modern communications requirements for electric generation sites including:

- Safe IT/OT integration
- ICS & turbine vendor remote monitoring
- Control center communications
- Protecting relay and safety networks
- Reduced NERC CIP V5 and V6 compliance costs

Given that unidirectional, stronger-than-firewall protections and architectures exist and are in widespread use, we all must begin asking: “which of our turbines, generators and indeed entire power plants are expendable enough to protect with firewalls and software alone?” The answer is self-evident. The time to act is now; the threat grows by the day.
Modern Threats

The electric grid has been identified as a strategic target for nation-state, terrorist, hacktivist and other attacks, and power plants are essential elements of the electric grid. Targeted “ransomware” attacks can encrypt control system components, triggering shutdowns long enough to tempt a utility to pay the attacker’s multi-million dollar demands. Hacktivists seeking to embarrass utilities or punish them for some imagined slight need only damage a handful of control system computers to trigger multi-day outages. More-sophisticated attacks on protective relays and safety instrumented systems risk consequences such as equipment damage, injuries and environmental damage.

Textbook, modern, network attacks begin with a piece of malware gaining a foothold on corporate networks, established by deceiving a power utility’s employee into downloading and running an attachment. The attachment is generally custom-written, so that no anti-virus, intrusion prevention, or intrusion detection signatures identify the attachment as malware. The malware typically tunnels a remote control connection to a command and control server on the Internet, by hiding its communications within a web application protocol the corporate firewall thinks it understands, and therefore allows. The attacker uses the remote control connection to compromise select additional machines, on the same network or deeper in the network architecture through layers of firewalls. In this way, the attackers are able to reach and interact with even those machines and networks that are configured to be unable to interact with the Internet. Once deep enough into their target, these attackers ultimately launch their end-game attack: either stealing information, shutting down control systems and entire plants, or even damaging rotating equipment.

These modern attacks routinely defeat all software protections, including firewalls, encryption, intrusion detection systems, anti-virus systems, security update programs, and strong password management systems.

Modern Attacks:

- Penetrate firewalls by spear-phishing,
- Evade anti-virus systems with custom malware deployed in volumes too low to trigger AV signature creation,
- Use professionals to operate sophisticated malware by interactive remote control,
- Gather passwords and password hashes,
- Create accounts on domain controllers and remote access systems, and then
- Log in to those accounts like any other user.
IT-Centric Security Not Enough for Power Plants

For years, IT-centric security has been held up as the “gold standard” for control system networks. This understanding is changing. Increasingly, experts recognize that IT-centric security fails to meet the needs of control system networks.

Traditional control-system defense-in-depth advice recommends firewalls, encryption, anti-virus systems, security updates and many other host and network hardening measures. A traditional, firewall-based network architecture is illustrated in Figure (2).

Traditional IT-centric advice recognizes that firewalls are porous by design; they forward messages from untrusted to trusted networks. IT-centric advice further recognizes that all software-based security mechanisms have vulnerabilities. All of this is why the pinnacle of traditional defense-in-depth advice is always Intrusion Detection Systems (IDSs) staffed by security experts, in effect “pitting our experts against theirs.” IT-centric advice encourages a determination to actively seek out compromised machines, contain them, identify stolen data, and restore the affected machines from backups.

An expert consensus is emerging which regards this traditional IT-centric advice as insufficient to address the threat of modern, cyber-sabotage attacks on power plants. The essential difference between IT systems and control systems is, not surprisingly, control. Control systems operate large, complex, dangerous physical processes. Damaged turbines and transformers cannot be “restored from backup.” Worse, intrusion detection, response and remediation take time: months for the average compromise. For all of this time, a remote attacker has control of our critical control and protection systems.

Modern advice for control systems recognizes that, while intrusion detection has a place in a defensive architecture, the foundation of the architecture must be intrusion prevention. Any malicious operation of plant equipment, however briefly, poses an unacceptable risk.
Modern Protections: Unidirectional Gateways

Advice for the protection of control system networks is being updated to reflect the stronger-than-firewall protections afforded by a family of technologies based on and complementing Unidirectional Security Gateways.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unidirectional Security Gateway</td>
<td>![Icon]</td>
<td>Unidirectional Security Gateways are used when data flows out of a critical network routinely, and when updates are required back into that network only rarely. Unidirectional Gateways permit data to flow out of critical networks into less-trusted networks, but physically prevent any attack, any message and any signal whatsoever from passing back into reliability-critical networks.</td>
</tr>
<tr>
<td>Waterfall FLIP</td>
<td>![Icon]</td>
<td>The Waterfall FLIP® is used when data flows out of a critical network routinely, and when updates must flow back into that network frequently and periodically. The FLIP is a Unidirectional Security Gateway whose orientation can periodically reverse. The FLIP hardware makes remote-control persistent targeted attacks physically impossible.</td>
</tr>
<tr>
<td>Inbound/Outbound Gateways</td>
<td>![Icon]</td>
<td>Inbound/Outbound Unidirectional Gateways are used when continuous data flows are necessary both out of and into critical networks. Two completely independent Unidirectional Gateway systems are deployed to support the continuous data flows.</td>
</tr>
<tr>
<td>Application Data Control</td>
<td>![Icon]</td>
<td>Application Data Control is a software add-on to all of the above products providing policy-based controls over industrial data flows, even for encrypted, compressed, proprietary and undocumented industrial protocols. This represents an extra layer of fine-grained control, in addition to the hardware-based unidirectional protections.</td>
</tr>
<tr>
<td>Secure Bypass</td>
<td>![Icon]</td>
<td>Secure Bypass is an electromechanical switch, able to electrically connect and disconnect two copper network cables. The default mode for the switch is the disconnected state. In reliability emergencies, the switch can be manually activated to permit conventional interactive remote access for the duration of the declared emergency.</td>
</tr>
</tbody>
</table>

Table (1) Unidirectional Security Gateway Technologies

Waterfall Security Solutions’ family of Unidirectional Security Gateway products all provide stronger-than-firewall protections for control system networks, and are designed specifically to defeat modern, professional-grade, targeted attacks.
Use Case: Safe IT/OT Integration

The most common use of Unidirectional Security Gateways in power plants is to enable safe IT/OT integration. The gateways generally replace unacceptably-vulnerable firewall-based integrations of networks and applications.

**Historian and Database Replication**

The most common unidirectional IT/OT integration architecture is a Unidirectional Security Gateway integrating plant IT and OT networks via a historian database, or relational database. When there is a historian or other database on the plant network, the gateway replicates the plant database to the corporate network, where corporate users and applications can query the replica without any threat to the control system network. When there is only an enterprise database, the gateways replicate Modbus, OPC and other servers and devices to the corporate network, so that the corporate historian or other database applications can acquire data from the control system data source replicas.

**Optional: Security Updates**

When regular anti-virus updates, WSUS or other security updates must be sent into the plant network, a Waterfall FLIP can be substituted for the Unidirectional Security Gateway. The FLIP provides for a disciplined flow of such updates into plant networks, without ever introducing the vulnerabilities that always accompany firewall deployments.

**Optional: SIEM and Other IT Integrations**

Waterfall’s Unidirectional Gateway-based products are often configured to replicate a variety of IT-centric data sources from plant networks to corporate networks as well. File servers can be replicated, to simplify reporting, debugging and other file transfers from plant networks to corporate and so minimize the use of removable media. Syslog servers and SNMP data sources can be replicated to Security Information and Event Management (SIEM) systems in corporate SOCs and NOCs. When branch SIEMs have been deployed on control system networks, Unidirectional Gateway products are able to replicate those branch SIEMs as well, aggregating plant information into an enterprise SIEM.

---

1 See IT/OT Integration Done Right and Done Wrong, UTC Journal, 2nd Quarter 2014, at [http://www.bluetoad.com/publication/?i=218589&p=19](http://www.bluetoad.com/publication/?i=218589&p=19) for a detailed example.
When additional protections are required to prevent data exfiltration, or to prevent malware from moving from plant networks to the corporate network, the Application Data Control option can be applied to the Unidirectional Security Gateway or Waterfall FLIP deployment.

Waterfall Security Solutions provides a wide array of both industrial and IT-centric replications in order to make Unidirectional Gateway deployments a seamless replacement for IT/OT firewalls.

**Security Benefits**

In all these examples, a layer of physical security in the form of the Unidirectional Security Gateway hardware is introduced between the high-risk corporate network and reliability-critical control system networks, breaking the online path of attack for attacks originating on the Internet or on other external networks. No fuzzing attack, no targeted remote control attack, and no virus or botnet however sophisticated can penetrate the physical protection provided by Unidirectional Security Gateways.

A related security benefit of this architecture is that with Unidirectional Security Gateway technology in place, there is no possibility that reliability-critical systems can depend on potentially-compromised IT systems, such as corporate Active Directory servers, DNS servers, documentation web servers, file servers and many other single points of compromise on untrusted corporate networks. Safe IT/OT integration via Unidirectional Security Gateways renders such unsafe dependencies impossible.
Use Case: Vendor Remote Monitoring

At most power plants, there is a need to support control system vendor “monitoring and diagnostics” programs. This is especially true for turbine vendors, since such vendors generally honor hardware warranties and support agreements only when the vendors have continuous access to vibration, heat distribution and other detailed data about the performance of rotating equipment. Turbine and other ICS vendors generally also require occasional opportunities to adjust control-system components to address problems as they develop, and so prevent serious failures later on.

Vendor Monitoring

Generating sites address this need by deploying a Unidirectional Gateway to replicate control-system servers from a reliability-critical network to a vendor DMZ. The DMZ is connected by the vendor to the vendor’s central management system, most often via a VPN across the Internet. The replicas are faithful copies of plant systems and provide the vendor full visibility into the status and condition of generating plant systems.

Optional: Remote Adjustment

If the vendor needs to adjust control system or turbine parameters from time to time, the vendor schedules time with site personnel. At the appointed time, site personnel sit down in front of a workstation with Waterfall’s Remote Screen View client installed, enable screen mirroring through a Unidirectional Security Gateway, and call the vendor. The vendor is able to view the screen of the plant workstation via a video feed streamed through the Unidirectional Gateway, without any ability to send any command or query into the workstation. The vendor is able to verbally guide site personnel through a process of adjusting the control system and verify that corrections have been made to the vendor’s satisfaction.

A secondary benefit of this approach to remote adjustment is that plant personnel are able to supervise the adjustment process. Plant records of such adjustments can bring value to any disputes with vendors over the management of generating plant assets.

Security Benefits

Vendor monitoring was traditionally enabled with firewalls and VPN connections. The VPN connections deployed between central vendor monitoring sites and generating units are encrypted, but encryption provides no protection from compromised vendor networks. Even connections claiming to be “monitor only” almost always enable the vendor software.
to query control system equipment for data, and are always over a bi-directional communications channel. A compromised vendor monitoring system can be used to pivot an attack across bi-directional “monitor only” links with buffer over flows and other malicious messages sent instead of legitimate queries.

Attacks work the other way as well - the central vendor site is itself at risk of attack from all control system networks to which the vendor’s site is connected via VPNs. Vendors make such connections in both the friendliest and un-friendliest of geographies, and to both the best-secured and the worst-secured control systems in their geographies.

With Unidirectional Security Gateways in place, electric generators are protected absolutely from compromised vendor machines and networks. The vendors can monitor the turbines continuously, but no network attack can reach back from the vendor’s central site into the power plant’s control system.
Use Case: Control Center Communications

Base-load plants frequently need to communicate with regional authorities such as the power utility’s generation-dispatch control center. The protocol of choice is often ICCP, but may also be any of DNP3, IEC 60870-5-104, or 61850 MMS. For some base-load plants, this communications is purely a reporting function; change orders from the regional authority are infrequent and are accomplished through schedules agreed to long in advance. Base load plants can be secured by outbound-oriented Unidirectional Security Gateways, as described in the IT/OT use case above.

Secure Control of Peaking Plants

Peaking plants are more complex. Peaking plants require continuous reporting to a generation dispatch center, and require a continuous, second-by-second stream of new setpoints from the dispatch center.

Unidirectional Security Gateways replicating the power plant’s ICCP slave or other protocol slave devices to a generating dispatch center meet the needs of some base load plants, and inbound/outbound Unidirectional Gateways can be deployed to meet the needs of all remaining plants. The outbound Unidirectional Gateway replicates the plant’s ICCP server to the corporate network or to a dedicated DMZ, so that the dispatch center’s EMS/SCADA master can poll the plant replica. The inbound Unidirectional Gateway replicates the EMS ICCP server back into the plant where plant systems query the replica for new setpoints.

Security Benefits

All control centers and generating dispatch centers are attractive targets for cyber-sabotage attacks. A compromised control center is able to mis-operate the grid, cause outages, and possibly cause cascading outages. A compromised control center can also be used as a platform to “pivot” attacks into partner utilities.

Unidirectional Security Gateways provide absolute protection from external attacks for plants that do not require continuous commands from a control center, and inbound/outbound gateway configurations are much stronger than firewalls1 for all other plants. For inbound/outbound configurations, the Waterfall’s Application Data Control option can be deployed for additional security, to permit only reasonable setpoint values to enter the plant control system from generation-dispatch control centers.

Use Case: Protecting Relay and Safety Networks

Safety equipment and protective relays are software components that are essential to modern reliability and safety programs. These components become ineffective when compromised, and so protecting these components is vital.

Secure Monitoring of Safety and Protection Systems

Unidirectional Security Gateways are routinely deployed to replicate devices from protection and safety networks to control networks for continuous monitoring. These replications use DNP3, IEC 60870, IEC 61850, Modbus and other protocol connectors. SNMP traps and syslog data sources may also be replicated to central Network and Security Operations Centers for additional reliability or security monitoring. Continuous monitoring is essential to all of security programs, process and employee safety programs, and electric system reliability programs.

These Unidirectional Gateway deployments may be the only unidirectional protections for the safety systems, or the gateways may be deployed as a second layer of security. In the latter case, the gateways protect safety systems from attack by plant insiders, and from attack by malware that may have reached reliability-critical control system networks via USB Flash sticks and other removable media.

Security Benefits

Unidirectional Gateways prevent all remote adversaries, no matter how sophisticated, from reaching through intermediate networks into protection and safety networks. With a plant’s protection and safety equipment safe from such attacks, utilities can be confident that even if some part of the plant’s control network is someday compromised, correctly-functioning protection and safety networks will ensure that no lasting damage can be inflicted to plant equipment, and no injury can be inflicted on plant personnel.
NERC CIP Compliance Benefits

The NERC CIP V5 and V6 standards both encourage the use of strong security in the form of Unidirectional Security Gateways by reducing the number of compliance requirements for unidirectionally-protected networks.

Exemptions From 30% of NERC CIP V5 Requirements

The NERC CIP V5 standards define External Routable Connectivity as “bi-directional” routable communications through an External Security Perimeter (ESP). Waterfall’s Unidirectional Security Gateways are never bi-directional. All communications are unidirectional, including inbound communications via a FLIP and Inbound/Outbound gateway pairs. A power plant protected exclusively by Waterfall’s Unidirectional Security Gateways therefore, has no bi-directional communications through an ESP, and therefore has no External Routable Connectivity.

<table>
<thead>
<tr>
<th>CIP Standard</th>
<th>Total Requirements</th>
<th>Secured By Waterfall / Exempt Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>002 BES Cyber System Categorization</td>
<td>7</td>
<td>-</td>
</tr>
<tr>
<td>003 Security Management Controls</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>004 Personnel and Training</td>
<td>19</td>
<td>15</td>
</tr>
<tr>
<td>005 Electronic Security Perimeters</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>006 Physical Security of BES Cyber Systems</td>
<td>14</td>
<td>11</td>
</tr>
<tr>
<td>007 Systems Security Management</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>008 Incident Reporting &amp; Resp. Planning</td>
<td>9</td>
<td>-</td>
</tr>
<tr>
<td>009 Recovery Plans</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>010 Change Mgmt &amp; Vuln Assessments</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>011 Information Protection</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>014 Physical Security</td>
<td>24</td>
<td>-</td>
</tr>
<tr>
<td><strong>Totals:</strong></td>
<td><strong>129</strong></td>
<td><strong>38 = 30%</strong></td>
</tr>
</tbody>
</table>

As a result, the power plant is exempt from the 38 CIP V5 requirements for Medium Impact BES Cyber Systems with External Routable Connectivity, precisely because the plant is not at risk from External Routable Connectivity. These exemptions in the NERC CIP V5 standards are designed to recognize the strong security afforded by Unidirectional Security Gateways to the power plant, and so serve to encourage the use of Unidirectional Gateways to improve cyber security and reliability. The compliance cost savings resulting from these


exemptions are substantial: up to millions of dollars per year. Statements from auditors in individual NERC regions have verified the legitimacy of these designed-in exemptions.

**NERC CIP V6**

The proposed NERC CIP V6 standards preserve all V5 definitions and exemptions relating to Unidirectional Security Gateways, and add new definitions and exemptions. CIP V6 again defines Low Impact External Routable Communications (LERC) as “bi-directional” routable communications. Unidirectional Security Gateways are physically able to communicate only unidirectionally, and so communications through a gateway never constitutes LERC. Unidirectionally-protected networks are exempt from all requirements related to LERC.
Cost Savings

It is rare for a technology choice to reduce simultaneously all of technology capital/operating costs, cyber-security risks/costs, reliability risks/costs and safety risks/costs. Unidirectional Security Gateways dramatically reduce all of these costs and risks when compared with firewalls.

**IT/OT Cost Savings**

The IT/OT interface is the most complex of the many network interfaces in a power plant. When a firewall is used to mediate this interface, that firewall must be maintained at a significant labor cost. To keep firewall configurations somewhat secure, firewalls require constant attention. Firewall rules must track corporate IP address changes, user/permission changes, and application connectivity changes. Since corporate networks change constantly, these rules and configurations change frequently, and every change to the firewall must be tested, reviewed, and documented, to ensure that no slip of the fingers has introduced vulnerabilities into the firewall configuration. Firewall IDS and AV signature subscriptions cost a large fraction of the firewall’s capital cost every year. Firewall logs must be monitored to identify intruders or insiders who may be testing account names or passwords, or enumerating paths through the firewall for future attacks. The unidirectionality of Waterfall’s Unidirectional Gateway deployments never changes; the gateways are set up to replicate a defined set of servers to the corporate network. Furthermore, even when a Unidirectional Gateway configuration changes, no change to the gateway’s software configuration can impair the security the Unidirectional Gateway hardware provides to the plant network. Gateway agent hosts can be managed as any other computer in the IT network, or in the critical network. No delayed software update or lost account password can put perimeter protection for the plant at risk. As a result, the labor, compliance and operating costs associated with Unidirectional Security Gateways deployed at the IT/OT interface are much lower than comparable costs for IT/OT firewalls.

**Other Cost Savings**

Additional important network interfaces, such as the interface to protection equipment or a connection to a turbine vendor, incur significant, on-going costs associated with operating firewalls that do not apply to Unidirectional Security Gateways. Firewalls forward messages from untrusted networks to trusted networks, and so are very vulnerable to attacks. NERC CIP V5 and other authorities require that firewall logs be monitored regularly to identify suspicious traffic that may be an attempt to find a path to forward malicious messages through the firewall. Unidirectional Security Gateways replicate servers. The gateways are not routers, they physically cannot support an inbound attack, and so do not require the scrutiny that firewalls require in order to try to deflect attacks reaching through network perimeters.
The Cost of Risk

No site is absolutely secure, least of all power plants protected by firewalls. When accounting for the cost of deploying and operating firewalls, corporate risk managers are required to count the annualized expected costs of security incidents, as well as more easily-tracked capital and operating cost outlays. Risk managers must account for the expected, annualized costs of all of:

- **Nuisance incidents**: security incidents impossible in sites protected by Unidirectional Security Gateways, where common malware enters a network through a firewall, or where unauthorized remote access or other unauthorized activities are discovered. Even if no site downtime is attributed to such incidents, there are significant costs associated with identifying compromised equipment, creating forensic images, restoring damaged computers and other devices from backups, and analyzing forensic images to determine how what paths through firewalls were used to attack the network, so that these paths can be remediated.

- **Downtime incidents**: security incidents where malware, unauthorized remote access or other intrusions compromise networks via firewalls, causing unacceptable performance or other impairment to compromised equipment and networks, and so triggered generating unit or plant-wide shutdowns. Such shutdowns can take significant amounts of time to correct, since the attackers and malware may persist in their attacks until forensic analysis is complete and the attack paths through the firewalls are closed off. Downtime incidents have all of the costs of nuisance incidents, plus all costs due to lost revenue, impaired reputation, and any fines levied for reliability impacts of the plant shutdowns.

- **Equipment damage incidents**: high-cost security incidents where rotating equipment, transformers, or other physical equipment are damaged in the course of attacks reaching through firewalls. Rotating equipment and large, high-voltage transformers may or may not be repairable. Costs include all of the costs of downtime incidents, plus all costs to repair or replace damaged equipment. Irreparably damaged equipment can take up to 6-18 months to replace.

- **Safety catastrophes**: high-cost security incidents, such as ammonia discharges or explosions, where workers at the site are injured, members of the public near the plant are injured, or where there are significant environmental impacts.

In short, corporate risk managers are required to attribute to firewalls all expected security incident costs that could have been prevented by deploying Unidirectional Security Gateways.
**Unidirectional Reference Architecture**

Cyber threats continue to become more sophisticated over time, and so best practices for cyber defenses must continue to evolve as well. The modern, unidirectional reference architecture for generation networks being described by a number of authorities is shown in Figure (7).

![Diagram of Unidirectional Reference Architecture](image-url)

**Figure (7): Unidirectional Reference Architecture**

In the architecture, every computer or other device that routinely accesses electronic mail, browses the Internet, or connects in any way to the Internet is regarded as “potentially compromised” and therefore untrustworthy. This “untrustworthiness” characteristic is transitive – any machine or device able to exchange messages with an untrustworthy machine, whether those messages are encrypted or not and whether those messages pass through a firewall or not, is also untrustworthy. In the figure, only the blue and green networks are considered trustworthy, because no equipment on those networks ever exchanges messages with untrustworthy equipment. Compare this with Figure (2) earlier in this paper, illustrating how “untrustworthiness” contaminates all networks connected directly or indirectly through firewalls to the Internet.

Unidirectional Security Gateway products in all their forms never forward messages, and provide hardware-based protections for plant networks. In this unidirectional reference architecture, no connection between a reliability-critical network and a less-trusted network...
is via a message-forwarding firewall. In this architecture, dangerous remote access paths have been completely eliminated. Permitting any machine on the Internet with stolen VPN and Remote Desktop passwords to log in and control critical equipment is an unacceptable risk. Even two-factor authentication is no help if the machine a legitimate user logs in from has been compromised. All software can be hacked, and a compromised laptop in a technician’s basement, or on a corporate network, can easily be used to attack reliability-critical generating networks.

Note that generation utilities may still carry out fine-grained segmentation of their OT networks using firewalls, provided these firewalls are used only to forward messages between sub-networks at the same level of trust. An example of such segmentation is the generating unit firewall in Figure (7) above.
Which of Our Control Systems is Expendable?

A decade ago, firewalls were effectively the only available technology able to protect our most important control system networks from corporate networks, central vendor sites, and the Internet. When we wanted to benefit from real-time access to control system data we had no choice but to connect networks, deploy firewalls and other security software, and “cross our fingers.” Today, cyber attackers have demonstrated repeatedly the ability to defeat all software-based security, including firewalls.

Waterfall Security Solutions invented Unidirectional Security Gateways to provide an alternative to firewalls for safe IT/OT integration. Today, Unidirectional Security Gateways are readily available, widely deployed, and documented as a best practice by leading cyber security experts, authorities and standards. Today it is possible to ask the question “which of our generating sites are so expendable that we can afford to protect them with software and firewalls only?” The answer is self-evident.

The risk-reduction benefit of deploying Unidirectional Security Gateways is clear – the reliability of our power plants, the very equipment in those plants, and the reputations of our generating businesses are at serious risk from modern attacks. To attack sites protected by Unidirectional Security Gateways, IT insiders, hacktivists, organized crime and even nation-states have no choice but to revert to physical attacks, whether by their own agents or by bribing or coercing an OT insider. This dramatically increases the difficulty in attacking generating sites, and this benefit is the reason that one authority after another is recognizing Unidirectional Security Gateways in their best-practice advice.

The impact of Unidirectional Gateways on most business practices is minimal. The impact of the gateways on truly unsafe business practices is to block those practices entirely – and this is precisely what we must do in order to secure our power plants. The Bulk Electric System will be measurably more reliable when Unidirectional Security Gateways are deployed more widely.

The case for securing our power plants with Waterfall’s Unidirectional Security Gateways is clear. The real question remaining is “when do we start?” Sooner is better. The threat grows by the day.
About Waterfall Security Solutions

Waterfall is the leading provider of strong network security products that protect the safety and the reliability of control system networks. Waterfall Security Solutions’ mission is to eliminate the use of firewalls in critical infrastructure control systems. The company develops products that provide stronger-than-firewall protections for industrial control networks. Waterfall’s products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and the Middle-East. Waterfall’s innovative products dramatically reduce the cost and complexity of compliance with NERC-CIP, NRC, NIST, CFATS and other regulations, and include support for leading industrial applications, including the OSIsoft PI™ Historian, the GE Proficy™ iHistorian, Siemens SIMATIC™/Spectrum™ solutions and GE OSM™ remote monitoring platforms, as well as OPC, Modbus, DNP3, ICCP and other industrial protocols. Frost & Sullivan describe Waterfall’s solutions as ensuring "optimum security for networks across user verticals" and awarded Waterfall the 2012 Network Security Award for Industrial Control Systems Entrepreneurial Company of the Year, the 2013 North America Award for Customer Value Enhancement, and the 2014 Award for Global Oil and Gas Infrastructure Security New Product Innovation. For more information visit: www.waterfall-security.com.

Please contact Waterfall directly for additional information on this topic or on any topic related to Waterfall products.