# Expendable ICS Networks?

*Evolving threats drive best practice security*

*July, 2014*
*Lior Frenkel, CEO & Co-Founder*
*Waterfall Security Solutions*

**Which part of our infrastructure is expendable?**
When most of today's best practices were documented, 4-5 years ago, security measures such as firewalls, VPN's, anti-malware, security updates, others, were seen by most practitioners as adequate protection from the then-pervasive, modern threats of the day: professionally-produced viruses, worms and botnets.

In the last half decade though, this assessment has been challenged. Traditional best-practice security technologies are all software-based. All software has defects, and some defects are security vulnerabilities. In practice then, all software and all software security technologies have discovered and undiscovered vulnerabilities. Today's pervasive, modern threats routinely defeat software security technologies.

In the last half decade, hardware-enforced security measures in the form of Unidirectional Security Gateways have come into widespread use, and are becoming part of best-practice guidance. With this industrial cyber security alternative now recognized as a best-practice, ICS security practitioners are increasingly asking "If software-based security measures fail to protect even IT networks from compromise, why would we use them to protect our ICS networks? Which of our ICS networks are expendable?"

**"None" is the right answer**
This is a serious question, because any incorrect operation of ICS networks is a threat to worker safety, to public safety, to environmental safety, to costly and difficult-to-replace industrial equipment, and to the reliable operation of important physical processes. In the case of critical industrial infrastructures, unreliable operation may, in addition, pose a threat to a nation's population, economy or emergency preparedness.

Again, the question owners and operators are seriously asking themselves is: "which of our ICS equipment is so expendable that we should protect it with only software?" These stakeholders increasingly conclude that "none" is the right answer – all ICS networks must be protected by at least one layer of hardware-based security defenses. Any equipment or physical process so unimportant that mis-operation or destruction by cyber adversaries is an acceptable risk, is equipment that should have been retired years ago.

**Protection solutions for modern threats**
Waterfall Security Solutions produces hardware-enforced security products focused on the prevention of cyber sabotage of ICS networks. Waterfall's products are deployed world-wide to protect everything from nuclear generators to refineries, offshore platforms and even geographically distributed systems, such as transmission substations and pipeline pumping stations. Waterfall's products are deployed because they reliably defeat network-based cyber-sabotage attacks, even the professional-grade, targeted attacks that routinely defeat firewalls and other software-based security protections.

## 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.

***Waterfall's Unidirectional Security Gateways*** are combinations of hardware and software. The hardware enforces security - no compromise of the gateway software can impair the security provided by the gateway's hardware. Unidirectional Gateway hardware includes a TX module that contains only a fiber-optic transmitter, and which is connected to an RX module that contains only a fiber-optic receiver. The hardware can send information out of an ICS network, but is physically incapable of sending anything back into the ICS network. This unidirectional 'feature' of the Waterfall gateway cannot be changed, circumvented or hacked. As a result, security that the gateways provide from network-based attacks is, unlike firewalls, absolute.

The gateway software replicates industrial servers to external networks. Users and applications on external IT networks can access the replicas for data, or query them for processed information, and can be confident of receiving the same answers from the replicas as the original control system servers would have provided. In this way, the Waterfall Unidirectional Gateway eliminates the need for access into control networks.

Waterfall's Unidirectional Security Gateways are deployed routinely as part of IT/OT integration efforts to integrate ICS and corporate networks, to integrate sensitive safety

Proprietary Information – Copyright © 2014 Waterfall Security Solutions Ltd. All Rights Reserved.

networks & equipment protection networks into control networks, and to facilitate modern 'industrial cloud' services.

***The Waterfall FLIP™*** is a Unidirectional Security Gateway whose orientation can be reversed. The FLIP acts as either a Unidirectional Gateway replicating servers out of an industrial network, or a Unidirectional Gateway replicating servers into an industrial network, but can never be both at the same time.

The FLIP is deployed in applications such as batch processing, where production orders must routinely be sent to ICS networks, and in substations and pumping stations, where continuous monitoring is essential, and where occasional, scheduled commands must be transmitted to these stations. Either way it is pointed, the FLIP is unidirectional at the hardware level. Unlike firewalls, the FLIP is physically unable to pass or tunnel TCP or other bi-directional connections through the FLIP hardware, and so no remote control attack can be mounted through a FLIP.

***The Waterfall Secure Bypass*** can be deployed in parallel with unidirectional solutions to enable full interactive remote access in emergencies. The secure bypass equipment can never be activated remotely by any network attack, however sophisticated the attack.

Secure Bypass is deployed on offshore platforms for example, which must be evacuated during hurricanes and must be operated by remote control from on-shore stations for the duration of such emergencies.

**Standards and Best Practices Are Evolving**

Owners and operators have invested significantly in cyber-security protections and rely heavily on best-practice advice. To be effective at providing the guidance which is essential for keeping industrial sites secure against pervasive and emerging threats, ICS security standards and guidance must continue to evolve.

Waterfall Security Solutions contributes actively to ICS cyber security standards and guidelines in many jurisdictions. Waterfall's objective is to ensure that widely-used guidance and standards effectively address modern threats, and accurately represent evolving best practices.

Unidirectional Security Gateways represent a new industrial security best practice, as cited by authorities including the DHS, NRC, NEI, ISA, IEC, NERC CIP, NERC ES-ISAC, and ENISA.

**The Bottom line – "None" is the right answer**

Owners and operators are encouraged to consider how expendable their control networks are. Today's best practices include hardware-based defenses for industrial control systems.

***Modern attacks routinely defeat software protections.***

***So – which of our ICS networks are so expendable that we should protect them with only software?***

**For More Information**

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

Waterfall Security Solutions
1133 Broadway, Suite 708
New York, NY 10010
+1 212-714-6058
info@waterfall-security.com

Proprietary Information – Copyright © 2014 Waterfall Security Solutions Ltd. All Rights Reserved.