State Based Network Isolation for Critical Infrastructure Systems Security

Wm. Arthur Conklin
University of Houston
waconklin@uh.edu

Abstract
The collision of information technology (IT) and operational technology (OT) networks has resulted in some significant security challenges. Cyber attacks are now taking place against critical infrastructures and the nature of industrial automation control systems equipment in OT networks makes traditional IT security measures more difficult if not impossible to employ. A new method of system isolation based on system state vice network traffic restrictions is presented as a means to protect critical systems from conventional IT based attacks. This new method of protection functions by isolating systems from the network, yet moving data in form of state transfer vice network message. This method improves reliability and provides a means of protection from most current IT based attack vectors.

1. Introduction
Recent history has provided some stark security lessons to the control systems network world. Industrial automation control systems (IACS) are used to control a wide array of cyberphysical systems, from manufacturing, transportation, energy, water, building automation and many more. These systems are called by many names, sometimes by industry, sometimes by functionality. Where information technology (IT) is known by most, these systems are frequently called operational technology (OT) and are known by few.

Some of the systems under control are either extremely critical or safety related. These systems have been around for decades, first in isolation, then they became networked into the enterprise in a quest for more timely data and control. The problem changed when risk and adversaries came knocking, with Night Dragon, Stuxnet and Duqu as recent examples. Cybersecurity has come to the IACS community, but it is not coming to a party it has attended before.

In the IT world, everything is connected in some way to everything. The Internet can and does carry virtually anything that can be packetized and does so without fail. This hyperconnectivity has created the Internet that we use every day, for shopping, communication, banking, even control over the Internet of Things. This has enabled many new things, apps for things we never knew we needed or wanted, but today can’t live without. And it created a whole new world for criminals and others who add risk to our daily life.

The result is also a degraded security environment for Industrial Automation Control System (IACS). These control systems were designed decades ago and do not have the security provisions found in modern networked components. Cryptographic mechanisms, strong authentication, security controls, the things we have developed over the last decade for IT systems are not available in most OT systems. One can argue the reasons why, but the state of the industry today is similar to the IT network 20 years ago, but with today’s current threat environment.

IACS engineers have a simple desire for their systems – reliability. It worked yesterday, it works today, they wish it to work tomorrow, so they do not like or want change. The enterprise has different desires from a business perspective. The business side desires more integration, both in data and systems. Integration of data into the enterprise can assist in the utilization of production data in real-time decision making. Integration of the systems can provide operational savings through tried and true IT principles of consolidation.

Isolation has failed in most IT cases as a security control, not because isolation doesn’t provide security, but because true isolation is difficult or impossible to maintain. Modern IT systems have a remarkable reliability record, and they have progressed significantly over the past decade with the use of virtual machines, automated systems for patching and redundant architectures designed to handle disaster recovery and business continuity. These gains have come from two decades of a three
year at best business generation cycle time, so today’s IT systems are 7th generation or better over the past 20 years.

IACS has moved at a much slower pace, with a cycle time measured in decades. Maybe one generation has really occurred in the same time period, and security has never been a driving concern. IACS network devices frequently lack the most basic security controls, authentication, logging, remote access, and cryptography. The lack of these underlying elements makes standard security tasks such as intrusion detection, forensics, incident response, even operational monitoring for things like virus and malware to be more challenging if not impossible.

The bottom line is fairly simple, these are not IT networks, they do not have the same level of sophistication, nor can they be operated like they are modern IT networks. They may be connected via internet protocol to other network elements, but they are not ready in a security sense for the standard IT security environment.

Isolation can work, as it has for years, but only if actually maintained. Isolation is not practical in today’s environment, but upon examination of what isolation means, this paper will present a means of isolating the system from network traffic will retaining the desired communication functionality. This will become increasingly important as these systems are just now becoming targets for adversaries, and will surely grow in importance both to us and those who wish to deprive us of their value.

2. IACS Networks

IACS networks serve a completely different environment than IT networks. The uses are different, the terminology is different, and the needs are different. Because of the systems they serve, IACS networks fall under a wide range of regulatory control based on the type of system and its criticality. Each industry has a set of applicable security regulations and standards. Originally defined by ANSI/ISA 99, and now IEC 62443, there exists a comprehensive set of standards for industrial control systems security.[1-3]

ANSI/ISA 99 introduces two concepts with respect to network architecture for security, zones and conduits. A zone is defined as a group of physical or logical elements clearly defined by a border that delineates included and excluded elements and that share a common set of security requirements. A facility can have numerous zones, each with differing purposes as well as security requirements. Communication between these zones is done via conduits.

A conduit is a delineated pathway for data between zones. Conduits act to control access in and out of a zone, both for data and risk. Conduits provide a means of managing security controls in a concentrated way vice having to do it for every element in a zone. For instance, malware scanning can be done by each device in a zone or at the conduits. Because of the lack of security controls available to most elements in a zone, conduits are where we place security controls that we want to cover the entire zone.

Conduits are not a new idea, they resemble the security demarcations of classic IT networks, such as firewalls and DMZ architecture. Beginning with a classic firewall based solution and advancing to a NGFW solution, conduits are the point of entry to a zone and require security resources to prevent bad traffic from entering or exiting the IACS network.

Unfortunately, both traditional firewalls and NGFWs have been shown to have limited usefulness against a wide range of attack vectors. For high value/impact zones we need a better control mechanism.

To understand what is needed, one must understand the IACS network and its function. A control system zone may have a bunch of new elements never encounters in a traditional IT network. Hardware elements of programmable logic controllers (PLCs), remote terminal units (RTUs), as well as other components such as intelligent electronic devices (IEDs). Software components such as human machine interfaces (HMIs) and data historians are also included. PLCs and RTUs are the devices that are physically connected to devices in the physical world. They are programmed using a variety of programming methods including ladder logic and assembly. The HMI is what an operator uses to issue commands to the devices, sometimes directly to the devices themselves, other times through a data acquisition computer. The data historian acts as a historical data record of all settings and readings reported by the devices. A whole new set of non-IP protocols are used to communicate between these devices. The IACS network exists to facilitate this communication between these devices.

3. Current Security Methods

One of the most commonly used methods to enhance security in systems is the air-gap. Breaking the network, not permitting traffic to and from a
device, or a group of devices is considered by many to be a gold standard. But air gaps have failed from a security standard time and time again. Stuxnet was designed to cross an air gap and did so with great effect.[4]

Air gaps are at best temporal gaps, not something to rely on for security. Air gaps are routinely crossed by operational purpose. The isolation from an air gap will be broken on purpose to obtain data, logs, and to deploy updates. When the air gap is bridged for these purposes, it is bridged for risk as well. The age of relying on air gaps to provide for security has long disappeared.[5]

Firewalls represent another security tool used to secure regular IT networks. Firewalls work at the network layer managing traffic. The challenge is in how you define evil vs. good traffic – at times a difficult task as there is no evil packet flag in packet header. Firewalls make their decisions based on other criteria, such as addresses and ports. As this has proven problematic in many advanced IT systems, the security community has responded with next generation firewalls (NGFW). NGFW operate by examining more deeply than just a packet’s addresses and ports, and can include stateful examination of packet contents. This has proven to be very useful in numerous types of traffic, to the point of allowing people to use a web application such as Facebook, but not an imbedded game within the Facebook application.

Next generation firewalls operate as application proxies and provide a wide range of valuable network services including inspection of files coming into the network, scanning for malware, blocking third party apps (Dropbox, Skype, webmail), blocking malicious traffic such as malware, botnets and remote command execution attempts. For an IT network, a NGFW can add significantly to the defense in depth posture. But in an ICAS network environment, NGFW’s have not been given the ability to separate good packets from bad in the control system network. They do not have the ability to recognize a Stuxnet type attack on a system.

Data diodes represent another method of limiting network traffic.[6] Data diodes are used to ensure one-way traffic in high security networks such as military networks. Designed so that traffic can only flow one way, a data diode prevents information from leaking out of a network while allowing data to be carried in. Data diodes solve a specific problem, they can block traffic from flowing in a single direction over a network path. But this does not address the security problems associated with IACS networks.

The underlying security problem is traffic. Internet carries all, even where and when it is not wanted or needed. And for IACS, they do not need to have any and all traffic traverse their network. IACS require a very minimal subset of all traffic and need the remaining traffic blocked.

4. New State Driven Security Model

One of the key security challenges is the separation of good traffic from bad or malicious traffic. The solution for control system networks is simple, stop letting traffic pass through the conduit. When examining what is truly required, network traffic is not on the list. What is desired is the passing of state from inside the network or outside the network, traffic is just a means of letting this happen. What is needed is a new model for the transfer of information through the conduit. In this new model, there is no passing of network traffic, only the state conditions associated with specific signals of interest.

Figure 1 illustrates a new model for network isolation, one driven by software.
An example: If we want to know the position of switches 1, 2, 3, and 4, then all we need to replicate through the conduit is the values for those switches. If we had a system in place on each end of the conduit, then what would pass through the conduit is only the state. If this is a one-way circuit going from the control systems network zone to some other zone, then in the control system network zone a packet encoded using the appropriate protocols could carry the state information to the edge of the conduit. At this point, the state information could be loaded into a state machine device that can encode the specific state and pass it through the conduit to another state machine device which takes the state information and reconstructs a packet to carry the information to a prearranged point.

Because all information flows are known, addressing is really a trivial issue done at setup. Because the only information being passed through the conduit is the values associated with the state of the system, the system is resistant to most known attack vectors. Assuming the code is clean from normal vulnerabilities such as buffer overflows, then the conduit state transfer mechanism is solid. Should either the receiving end or the transmitting end suffer from an exploitation of a vulnerability, the result will be failure and potential denial of service. Other failure modes will be prevented though the hardware/software combination that manages state across the conduit.

This communication across the conduit is performed using a unidirectional gateway. This is a combination of hardware and software designed to replicate state, not pass traffic. Just as whitelisting provides positive control over what runs, this solution gives positive control over what is transferred. Moving the data via a hardware/software solution that only moves the required information and nothing else prevents any other information streams from passing.

ANSI/ISA recently adopted the term unidirectional gateway in its security documentation. These devices are typically a combination of hardware and software specially constructed to operate in a manner to achieve isolation across the conduit yet pass state.

This provides for a method to move state without passing traffic in or out of the network. Although possible to collapse the network via a denial of service attack, the endpoint of the conduit will either be the state information or nothing as other values are precluded by the system setup.

5. Theory

Why does this solution improve security over existing security solutions? Two reasons, reduced attack surface and reduced system control surface. The attack surface presented to an attacker are the two ends of the conduit. Attack the end where the data enters and the state will not be properly replicated preventing transfer. Attack the end outside the IACS network and one can collapse the system that creates packets from the internal side of the conduit. Damage to the conduit exit point only causes the data being sent out to be lost, a form of DoS.

Attack patterns and data are both carried by network traffic. What is desired is to pass the data (state) and not any of the attack patterns. This solution separates the data from the network traffic. Unidirectional gateways can be built that can manage multiple sets of state communications data and log information from the system.
The design of the gateway is such that the only thing that is moved across the conduit are specific states predetermined during the setup/configuration process. Any other data is left behind as it does not fit into the state-transfer model. There is no attack surface presented in the conduit itself, only on the side of the conduit in the direction of flow. And then the only attack surface is one that would be susceptible to denial of service, just as if a cable was cut.

The second reason behind why this improves risk is related to the science of system regulation. The conduit can be considered a system with an input, and an output. Regulating the system is the mapping of state conditions from the input to the output side of the conduit. The Law of Requisite Variety can be applied to this simple system with the input to output mappings being the regulator controlling the system. A system under control must have a regulator that is at least as complex as the states under control. [7]

The original conduit method, with all of the possible internet traffic passing as well would make this regulator have to scale with the increase in signal diversity. A control system channel, with its limited number of states to be transferred would need a significantly smaller regulator than a channel with Internet traffic as well. So, the Internet, with its carry any and everything, nearly infinite number of states is basically uncontrollable.

Reducing the size of the regulator function makes control not only possible but more likely to achieve desired results in determining deviations from normal conditions. By removing any traffic other than that carrying the states in the control system network, on can dramatically improve other security operations efficiency. When the network is actually clean, then the diversity of the traffic is limited making detection of traffic outside norms easier to detect and remediate. Also, by blocking out traffic by type, such as SMTP traffic, then if it ever should appear on the IACS, it can be alerted on as it is surely an error.

6. Operationalization

The novel concept of transferring only state is of little use unless it can be operationally implemented in real systems. To implement the idea will require three steps. These steps are; define information transfer needs, architect zones to support information flow isolation, and connect to conduit via unidirectional gateways.

The first step, defining information transfer needs is the most critical as it defines the starting point for all of the steps that follow. A failure to capture a specific need will result in one of two outcomes, the data is never available, or a secondary, unprotected access channel will be created to transfer the data. Both of these represent a failure in the design and implementation, so this step requires significant study for completeness.

A key step in defining needs is the complete definition of all required data flows in and out of the zone via the conduits. Examples of information flows to consider include:

- Data (Historian) to Enterprise
- Log data to enterprise
- Updates to computers in zone
- Updates to control system equipment in zone
- Admin updates (AD, DNS) in zone
- Maintenance connections to devices

Defining the required traffic flows is the beginning, for once the traffic is determined, it is necessary to get into the specifics. As the last step will be the transferring control to state transfer devices, each set of states needs to be defined.

What about other common traffic types like HTTP, SMTP, and all those other “useful” protocols? The real question is why is this traffic on the control system network in the first place? If it is needed in the control room, then why not use a separate network segment, moving this activity into a separate zone.

Cleaning up zones of systems with actual differing security needs can assist in the securing of the zones via conduit channels. Move all non-control system stuff to a separate network segment (zone). For instance, if you use an Internet based weather service, then keep this in a separate zone and not mix this internet traffic with company control system traffic. The same technique can be employed for an engineering workstation used for checking email?

The next step involves securing the conduit. Replace the conduit network connection with a set of state transfer devices on each side of the conduit. Unidirectional gateways will be configured to pass each channel of states as identified earlier to pass state though the conduit. This multichannel approach is illustrated in Figure 2.
Figure 2: Separate Zones

This is not a data diode solution, as it is not about one-way traffic regulation. Unidirectional gateways must understand state for the data being passed. Because there will be multiple channels in and out of the conduit, multiple gateways will be required, one for each unidirectional channel. Figure 3 illustrates this setup.

Figure 3: multichannel/multidirectional data transfers.

There are vendors in this space, but the solution is not achieved by buying a piece of equipment. The solution comes from thinking differently about traffic and the requiring that traffic be excluded from sensitive network areas.
7. Effectiveness

The effectiveness of this method in reducing risk from security issues stems from its ability to isolate the system from traffic containing attacks. In this model, there is no direct attack surface pathway to systems from the outside. This has the advantage of rendering most attack patterns as ineffective.

Examining some samples of current attack patterns yields the following results. Assume an inbound conduit from outside the control system zone to inside. The conduit has a state transfer mechanism for transferring system updates into the control system network. An attack from Stuxnet would present no state information to the incoming side of the conduit, so no state would be passed in. Heartbleed attack, same result. Buffer overflow attack – if the incoming client on the conduit fell prey, the result would be DoS. If the incoming side did not have an exploitable vulnerability, no states would be passed and the system would pass nothing in. Race condition, same result. Injections, same result. APT dropper, same result.

Virtually all of the top 25 vulnerabilities can be addressed in this fashion. The only attack vector left open is related to denial of service and these are virtually impossible to stop in today environment.

8. Analysis of Alternatives

Where does this new model fit? Certainly not with all IACS systems. Isolation via state determined communication over unidirectional gateways is a technique that is for the cases with the highest risk profiles. Critical infrastructure systems supporting safety critical systems, health or systems that we cannot afford to be without fall clearly into this category.

Examining alternatives give note to a couple common practices. Air gaps, the first line of defense in many minds were covered earlier in the paper. They are temporal at best. VPNs are another common response. By their very nature, VPNs address the wrong problem. VPN’s do not limit traffic to or from a network. Instead, VPNs expand a bubble around a specific device, including it as if it was internal to the network. When you connect a machine in via a VPN, you get everything from the machine in, not just what you wanted.

VPNs will be a part of a complete security solution associated with a control system network, they are just not the part of the solution that is enforcing signal isolation. Even with the signals going in and out of the controls network being isolated via state transfer, it is still appropriate to employ other security controls in a defense in depth strategy. The use of application whitelisting on all of the machines, at least those that can use whitelists is an important layer of defense. Employing IDS systems to alert when unauthorized traffic is present is another. Blocking of USB ports on all machines to prevent data extraction or network cross connection from charging cell phones is another logical step.

9. Future Directions

This research presents a new novel method of isolating high value targets via a state transfer mechanism. Although highlighted for use in industrial control systems, this same technology can be employed in other high value targets including isolating point of sale systems, off shore oil platforms and systems that are stuck with older vulnerable OS’s like XP.

Although initially this solution is presented as a series of individual, separately configurable unidirectional gateways, the implementation could be reduced to a form of a bump in the wire where specialized ASICs could be employed to manage the defined state transfers.

10. References

3. ANSI/ISA, 62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels. 2013.
5. Richardson, C., Bridging the air gap: an information assurance perspective. 2012, University of Southampton.