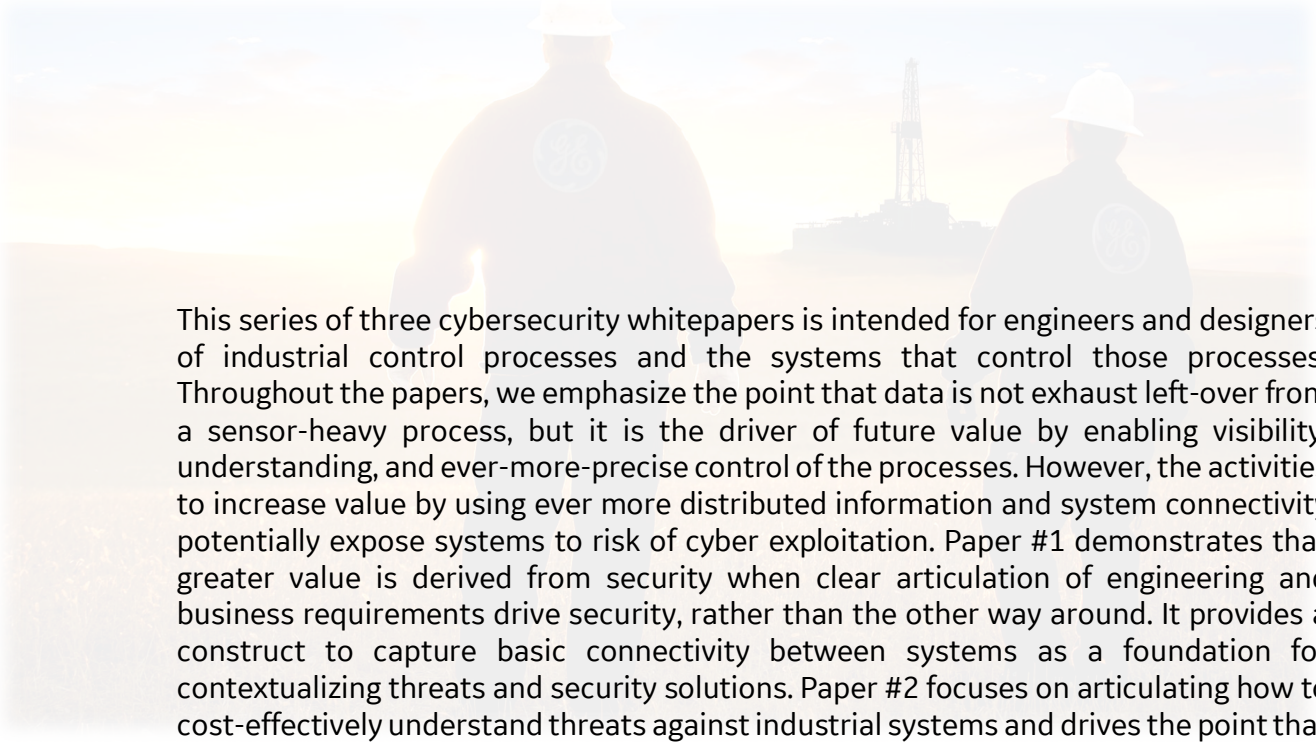
2018

Building security to achieve engineering and business requirements

DESIGN AND BUILD PRODUCTIVE AND SECURE INDUSTRIAL SYSTEMS, WHITEPAPER #1

KENNETH G. CROWTHER (GENERAL ELECTRIC), ROBERT M. LEE (DRAGOS), K. REID WIGHTMAN (DRAGOS)

A COLLABORATION BETWEEN GENERAL ELECTRIC AND DRAGOS.



This series of three cybersecurity whitepapers is intended for engineers and designers of industrial control processes and the systems that control those processes. Throughout the papers, we emphasize the point that data is not exhaust left-over from a sensor-heavy process, but it is the driver of future value by enabling visibility, understanding, and ever-more-precise control of the processes. However, the activities to increase value by using ever more distributed information and system connectivity potentially expose systems to risk of cyber exploitation. Paper #1 demonstrates that greater value is derived from security when clear articulation of engineering and business requirements drive security, rather than the other way around. It provides a construct to capture basic connectivity between systems as a foundation for contextualizing threats and security solutions. Paper #2 focuses on articulating how to cost-effectively understand threats against industrial systems and drives the point that security should be adapted based on connectivity requirements from the business and the threats to the processes, rather than published vulnerabilities and exposures. Paper #3 ties the two pieces together and further explores details of how engineers can guide the implementation of good industrial control system (ICS) security into the future as next generation control systems and connectivity requirements emerge. It assumes some knowledge of the basics, and focuses on what engineers should learn to design next-generation security around the business and engineering requirements of ICS.

Outdated or Unknown System Information Wastes Money

Better System Knowledge Decreases the Costs of Capital Investments and Accelerates Operational Troubleshooting and Response

Outdated system information increases capital and operating costs. For example, if planning a $10 million upgrade, you might spend 100-200 manhours to update piping and instrumentation diagrams (P&IDs) to avoid the risk of an extended outage which might cost millions. When trying to lean-down water or energy consumption, increase yields, or just bring a system back online quickly, outdated P&IDs can double or triple the time to resolution, and decrease the probability of success.

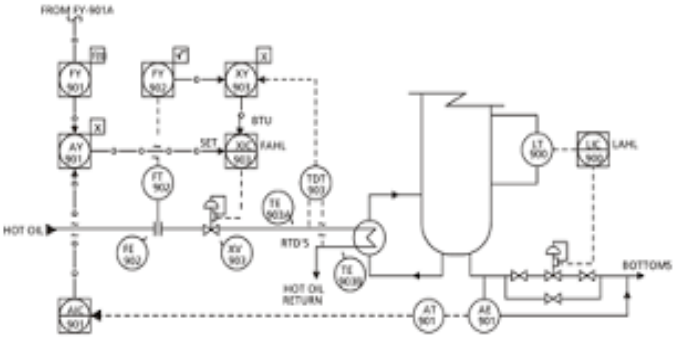


FIGURE 1. EXAMPLE P&ID SHOWING SENSORS, CONTROLLERS, AND DATA LINKS IN AN INDUSTRIAL CONTROL SYSTEM.

Understanding process and operating conditions is key to designing profitable industrial processes. As industrial processes evolve, sensors provide opportunities for increased visibility into process; data integration and analysis improve our understanding of process; machines become more capable of control; data connectivity becomes increasingly possible; but traditional enterprise network security may be in conflict with emerging business needs for industrial control processes. For example, a few tenants of traditional information technology (IT) security are segmentation (isolate systems and their information), least-privilege user-access (isolate people from systems information), product patching (update software and hardware), and encryption (reduce visibility of system data). In the IT security space, tight relationships have been developed between the businesses and IT security, so that security is carefully built around business requirements. In industrial systems, we have noted some conflicts that resulted in either sub-optimal security and vulnerable processes or good security at the costs of suboptimal process or unnecessary security expense. We need better collaboration between process designers and engineers, and the security teams that help protect industrial control networks. This will become increasingly important as IT merges into the industrial operations environments in an Industry 4.0 or Industrial Internet of Things (IIOT) era. This paper focuses on the idea that the first key to good security is a clear understanding of engineering and business requirements – to build security to achieve those requirements might require innovation beyond IT security traditions.

Consider the following illustrative examples where engineering requirements make business sense but may require security innovation through collaboration between engineers and security experts.

A POWER COMPANY CAN MAKE AN EXTRA $100 MILLION BY CONNECTING CONTROLLERS TO EXTERNAL DATA.

Unoptimized operations of an 800 MW plant would potentially lose money 50% of the time because of the fluctuations of gas and electricity prices.[1] Operators monitor prices and make operational decisions, but it is complex to compute optimal combinations of price margins, operating profiles of turbines, and the impact of current operating decisions on future maintenance costs.[2] When the turbine makes optimal operating conditions in the context of market, operational, and maintenance information it can potentially increase revenues by $100 million per year. Traditional IT security would promote network segmentation and would look disdainfully on connecting a turbine controller to the outside Internet for market price data, but full segmentation would result in missing a control network requirement with a business need. The connection must be secured, but knowledge of connections and careful design can assure that only valid information is changing processes.

A PETROCHEMICAL COMPANY CAN MAKE AN EXTRA $17 MILLION BY PREDICTIVE MAINTENANCE.

Offshore oil and gas organizations experience on average $49 million in losses annually due to unplanned downtime, which has been reduced by 36% ($17 million) with a data-based, predictive approach to maintenance.[3] Operators do not have the expertise for this type of analytics; it requires control networks to push data to sites for 3rd party access, and potentially run sophisticated scripts that are difficult to code into ladder logic. Traditional IT security would promote least-privilege access and layered segmentation and restrict running scripts in the control network, which create additional expense and delays in analytics and might miss the full benefits of timely predictive analytics. The 3rd party access means the business and its security staff may not be aware of a breach at the 3rd party where an adversary could leverage the information to tailor a cyber-attack. Compensating controls of a more robust threat monitoring and response program could be put into place instead of denying the business requirements. Additionally, the safety system in this organization becomes more important due to remote cyber threats; better segmentation for safety sub-systems would be an additional compensating control. Better processes for strictly defining collaboration and monitoring of utilization by various roles will become important to engineer business opportunities.

A MINING OPERATION CAN MAKE AN EXTRA $10 MILLION BY ADDING ADDITIONAL SENSORS TO EQUIPMENT.

Mining operations are remote and typically spend weeks per year with equipment outages due to time required to report, call for service contracts, ship specialized parts, and bring out specialists to make repairs. Putting sensors on equipment, establishing a network to share equipment status, and establishing processes for monitoring and predicting maintenance, can result in potentially $10 million in cost reductions, productivity improvements, and down time reductions.[4] Traditional IT security would promote encryption and device signing, of which few sensors specified for the remote mine are capable, but refusing the equipment monitoring at the remote mine would result in missing the opportunity for savings. The application of encryption is seen as a panacea, but encryption protects the data from view and can make security monitoring more difficult if applied incorrectly. However, we can still encrypt point to point from the gateway to the monitoring company, even if we don't encrypt at the remote mine. This will enable secure remote monitoring of equipment to enable business requirements but will require processes to cross-validate sensor signals. Device signing is an important security topic where possible, but additional approaches such as threat monitoring can compensate for the lack of device signing on sensors. The point is to tailor security to business requirements.

Engineers working with their business leaders should recognize and push the requirement for connectivity, access, and sharing of sensor data – *when it makes engineering and business sense*, and when compensating security controls are applied to reduce any new risks introduced. Security can, and should, be tailored around these engineering and business needs. Engineers and designers should also look to work with their security team(s) to build non-intrusive security into the industrial control system (ICS) which will produce more value than relying simply on later bolt-on solutions. This will require engineers to understand these connectivity needs and cybersecurity threats. It will also require two-way communication and collaboration between engineers and security professionals.

What happens when you are pitching a new concept to the Plant Manager or CEO and IT Security calls for security in a way that completely prevents the implementation of new business concepts? For example, imagine that IT Security throws a thick copy of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 on the table and states that this list of controls is expected by all information systems, which could forbid your proposed engineering advancement. How do you respond? One possible answer would be to explain how cyber security standards were constructed as a generic guideline to apply to most information systems. These controls can be implemented around new engineering requirements that create significant value from interconnecting data, but we need to tailor and innovate new ways to apply the controls – as the standards recommend.

The rest of this paper describes a foundation for communicating and initiating this collaboration with IT security professionals. The second paper will discuss how to understand threats against ICS, so that engineers and process designers can better understand the security tradeoffs that are reasonable to make. The third paper in this series connects design requirements for connecting systems for data-movement and the emerging threats to ICS that exploit those connections to provide an evolutionary path to continuously improve security.

ENGINEERS CAN LEVERAGE THE PURDUE MODEL TO COMMUNICATE AND COLLABORATE WITH CYBERSECURITY EXPERTS

In the 1990s, T.J. Williams suggested expanding the Purdue Enterprise Reference Architecture to incorporate the connection of information technologies with manufacturing process. In short-hand, this model is referred to as "the Purdue Model." The Purdue Model was intended to be flexible, but its encoding into standards such as ANSI/ISA-95 and IEC 62264 has given the impression that it is rigid and well-defined. It provides foundational language for control systems security standards like IEC 62443 and NIST SP800-82. The basic idea (and the way that it was originally proposed) is easiest to digest if we think of an enterprise as a centrally run and top-down hierarchy that is decomposed into five levels. (Enterprises and operations used to be architected in this hierarchical way; we present later how this can be applied to modern ICS.)

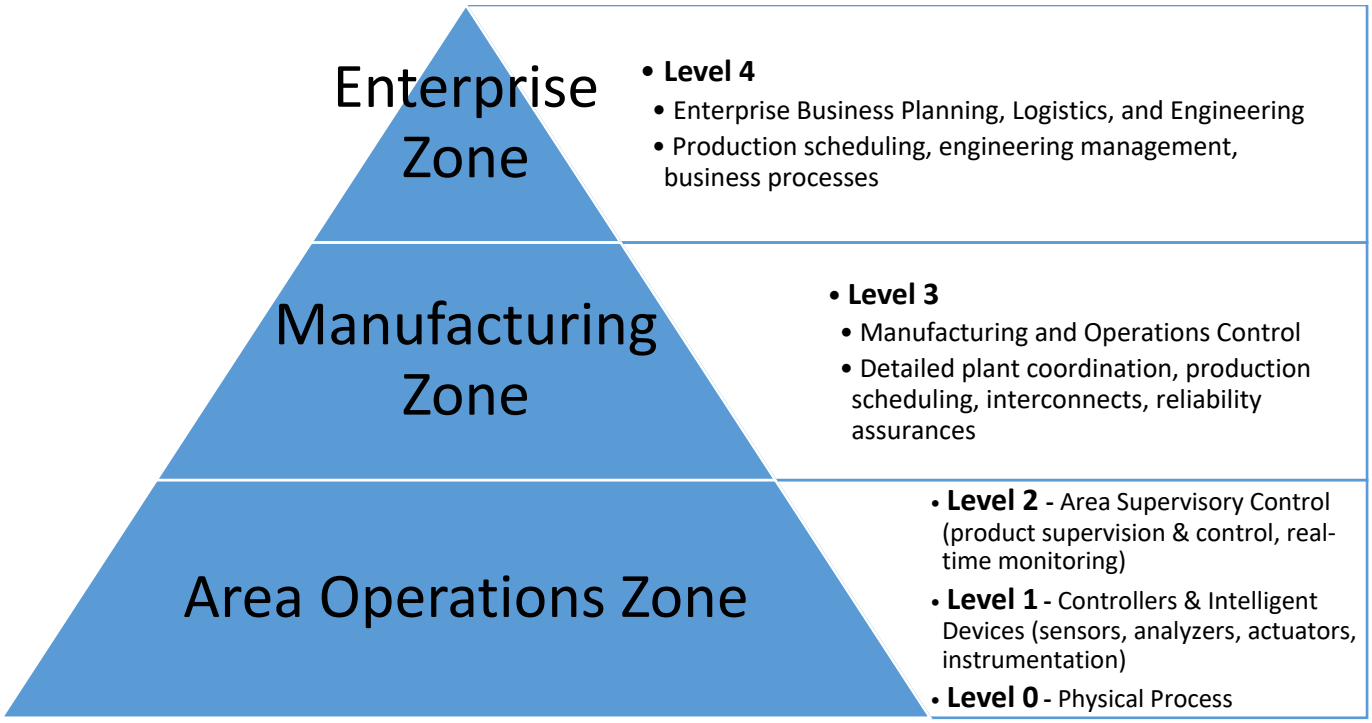


FIGURE 2. THE TRADITIONAL PURDUE MODEL STILL PROVIDES A FOUNDATION FOR MODERN INDUSTRIAL SYSTEMS.

Even though many industrial processes are increasingly non-hierarchical, especially as we evolve to IIOT or Industry 4.0, the core tenants of the Purdue Model are still useful for laying a foundation to discuss cybersecurity.[5] For example:

- Connectivity and security requirements may be deployed similarly within a level, but different across levels.
- Devices within a specific level are generally trusted, but connections across levels should not be trusted and should require additional layers of security.
- Value is derived when upper layers exploit information generated in the lower levels (e.g., Level 3 needs data from Level 2 operations to reduce resource use and improve production rates).

While the Purdue Model is quite flexible, it is difficult to describe the complex connectivity of modern systems in this hierarchical version of the model (sometimes called the "wind-chime" model).

Understanding your architecture is the first step toward being able to discuss securing your system. Does the Purdue Model still work?

The reason many find it difficult to apply the Purdue Model is that the original application of the Purdue Model was created when most production systems were isolated and weakly connected outside of the enterprise. Modern industrial systems are increasing autonomous (machine-centric), connected (data moves, is integrated, and analyzed), and accessed by more diverse roles for tuning and optimization. Figure 3 provides a high-level "sliding scale" of connectivity. The Purdue Model can apply to the entire spectrum but may look significantly different than the wind-chime version above, as we move across the scale toward increasing connectivity.

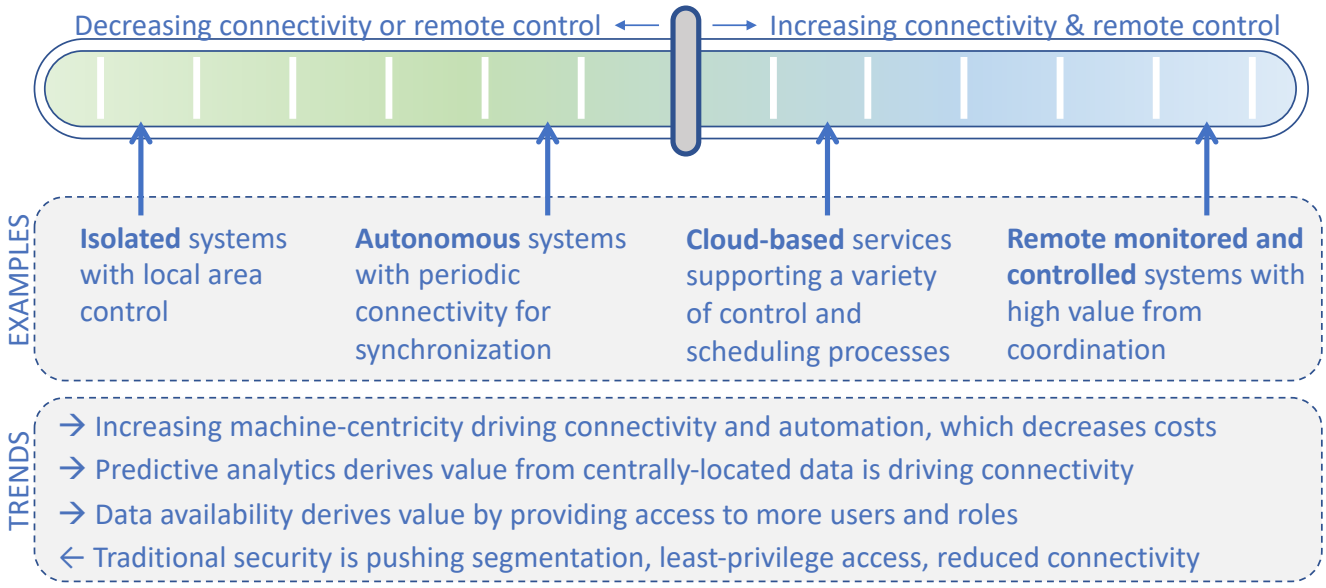


FIGURE 3. ICS EXIST ON A "SLIDING SCALE" OF CONNECTIVITY, TRENDING TOWARDS GREATER CONNECTIVITY AND REMOTE CONTROL.

While numerous processes with low connectivity requirements (on the left side of the scale) still exist, information and technology are emerging that enable cost savings or additional revenue from collection and exploitation of information. The ICS community has devices that can sit on the edge of networks to secure connections to outside data and even accelerate algorithm processing by running complex scripts not feasible with traditional controllers. Indeed, even though data used to be viewed as exhaust of the system, it is now understood as the central value-generating feature. New opportunities for advanced network security exist for control systems, such as software defined networking technologies that enable dynamic network security requirements. The ICS community is learning from the IT community that network perimeters which trust devices to indiscriminately connect laterally across the network result in exploitation. These communities are enabling secure connectivity through ideas such as micro-segmentation and continuous monitoring. As our evolving Industry 4.0 ICS take more advantage of IIOT technologies, we will be dealing with requirements for connectivity, access, remote control, and data sharing. It is important that these requirements drive new security and are deployed in collaboration with security engineers, rather than have security forbid the requirements or deploying without security because of the inability for engineers to collaborate to lead security solutions.

THE PURDUE MODEL APPLIES TO MODERN SYSTEMS, BUT ENGINEERS NEED TO LEARN HOW TO USE IT.

As our ICS move to the right on the sliding scale more of our data and processes are interconnected and exposed. For example, electricity transmission and distribution (Purdue Level 0) have interconnections across enterprise ownership, which can result in cascading failures and uncertain load. Some power generation systems have controllers connected to external databases that can adjust control (Purdue Level 2) based on market price predictions. Logistics systems across corporations and enterprises capture and send logistical data from the operations site (Purdue Level 3) to reduce wasted resources and inventories. A modern interpretation of the Purdue Model that accounts for the reality of increasing interconnectivity and security would build on the concept of a "service bus" that provides a platform of interacting parts with some sort of common data and communications capability that enables interconnectivity, and would add the concepts of Edge and Cloud services to capture the reality of connections across enterprise boundaries that might not go through the enterprise network. Figure 4 is an example of a Purdue Model for an ICS on the right side of the sliding scale of connectivity. This type of model will allow for high levels of connectivity, but will also demand new and innovative approaches for security that continuously monitors and is based on device and identity states.

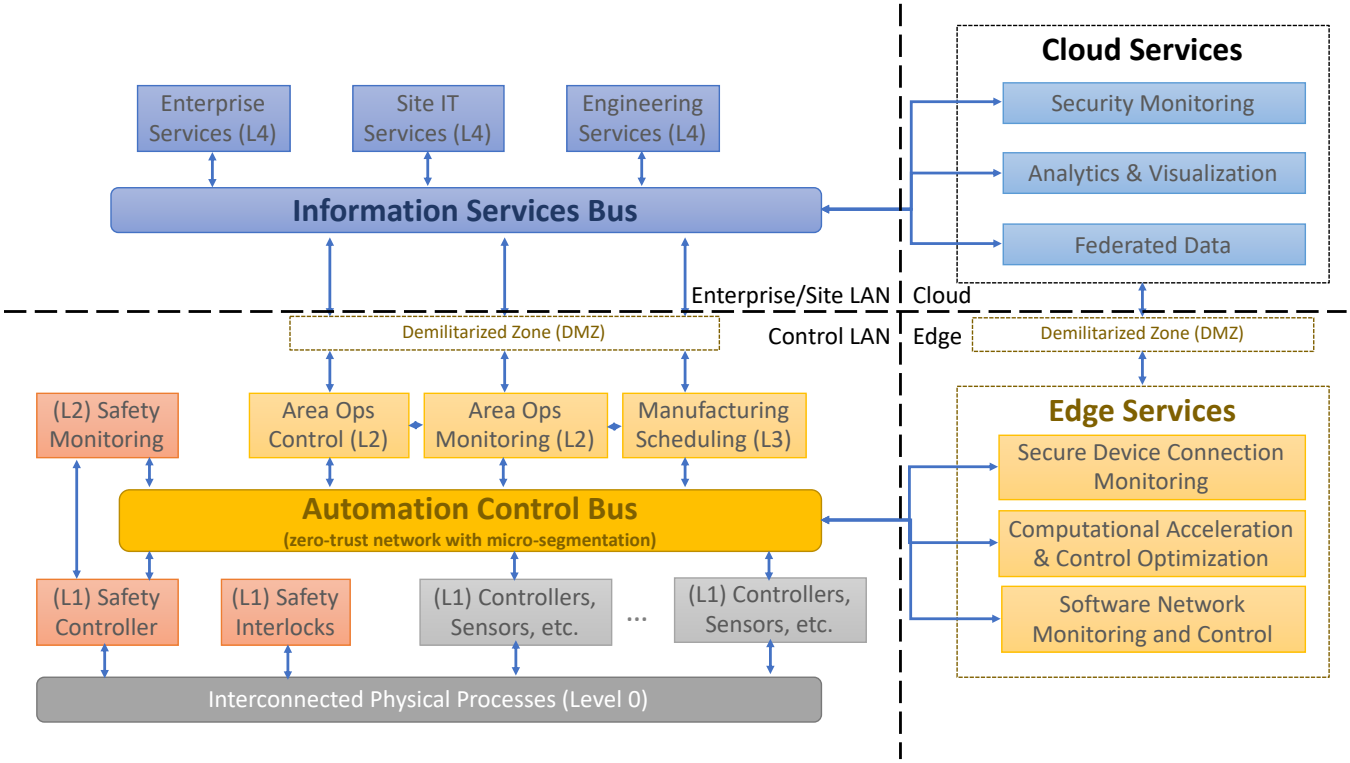


FIGURE 4. APPLYING THE PURDUE MODEL TO A HIGHLY CONNECTED SYSTEM MAY LOOK DIFFERENT.

Some key changes make this version of the Purdue Model less recognizable:

- Interconnected processes (e.g. electric grids and connected additive manufacturing) emphasize the reality of not being able to fully isolate system control for process segments. Optimizing control will require increased connectivity, but will also enable security innovations

that can, for example, compute improper sensor reads or out-of-bound commands based on computations from orthogonal process measurements and controls. Imagine a monitor that is constantly checking for process consistency based on the chemistry or physics of the process – it would require very complex sequences of process manipulations to hack ICS and would substantially increase the cost to adversaries while also improving safety.

- The increasing functionality and intelligence of sensors, actuators, and drives, and their integration with protocol standards (e.g. TCP/IP, OPC, Modbus, BacNET,) has flattened the architecture of automation sites. It appears more like an automation and control service bus that allows interconnectivity instead of a hierarchically designed control system. As such, the lines between Levels 1, 2, and 3 have started to flatten. This potentially enables traditional security stacks to work on ICS networks with modifications, but it will demand a move toward "zero-trust" philosophy in which each device and identity will need to be screened and monitored. This will demand dynamic networking capabilities, more-sophisticated connection policies, and technologies that will support this in a zero-down-time environment.
- The increased use of standard features and protocols have enabled integration of IT equipment (switches, hubs, servers) into the automation and control network. This will shift bandwidth and reliability capabilities, perhaps requiring additional computational capacity on the edge of control networks.
- Information technology has also shifted toward data and communication standards. What used to be a highly planned architecture of an enterprise, now increasingly relies on wrapping functions and data to provide them "as a service." The automation and control systems are still separated from the enterprise operations by a demilitarized zone (DMZ). This allows for the enterprise functions to benefit from the operations data for improved scheduling, engineering, process optimization, and so forth. This also enables behavior baselining and improved detection of out-of-bound activities on the network, while still allowing for emergency actions and rapid response.
- Virtualization, network control standards, and modern switching speeds enable tailorable zones defined dynamically through software defined networks, instead of static firewalls and physical switch-based zoning. Zones may be less clearly defined along traditional Purdue Model levels and instead defined around information connection requirements.
- The increased ability to tailor network zones enables new capabilities on the network edge to accelerate algorithm processing for data-intensive control, connections of lower-level devices to external data, and provides opportunities for security monitoring of the automation network layers.
- The shift in the reliability of automation networks has driven the need for maintaining some isolation to safety systems. In some cases, these are still mechanical, electrical, or pneumatic control systems that operate semi-independently of the network. The engineering of these safety controls and interlocks should expand their design baseline –they should consider potential adversarial tactics in addition to traditional safety or error considerations. These safety systems become increasingly important to segment and protect as the entire control networks become more integrated, connected, and remotely controlled.

Admittedly, no single vendor or integrator provides all of these technologies in production-ready form (including the authors). However, each of these technologies currently exist or have active pilots by various vendors. The standardization and service reorientation of both enterprise and automation capabilities has resulted in the emergence of edge services for securing the automation control bus,

enhancing analytics, and providing new possibilities for optimizing control. The first step to engineers enabling a profitable, efficient, safe, reliable, and secure system is to understand and represent data connectivity requirements and how they require connections between controllers and other devices across the network. The Purdue Model still provides a foundation, but it needs to be tailored to adequately represent interconnection requirements for tailored segmentation, least-privilege access, and secured channels of communication. The more the engineers can understand and represent these features, the better they will be able to work with cybersecurity practitioners to enable their systems while securing them.

This whitepaper is followed by two additional papers. Paper #2 (*Understanding threats will promote the "right amount" of security in industrial systems*) focuses on understand threats to your systems and how to use threat information to tailor security in the engineering and operations processes, and Paper #3 *(Blending resilience and security hardening will achieve the greatest security for the most business viable systems*) focuses on developing security and resilience into your systems to accomplish your connectivity requirements in a secure and resilient way.

RECOMMENDED FURTHER READINGS:

1. Luciana Obregon, 2015. *Secure Architecture for Industrial Control Systems.* SANS Institute InfoSec Reading Room. Available online: https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327. Obregon connects modern ICS security practices to the Purdue Model – so if you learn your architecture from the Purdue Model perspective then you will be able to quickly identify security requirements to start enforcing.
2. National Institute for Standards and Technology (NIST) Special Publication 800-82 Revision 2. *Guide to Industrial Control Systems (ICS) Security*. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf. NIST provides several example architectures of systems and describes a general process for understanding your architecture, evaluating your risk, and selecting controls for your process.

---

[1] For example, see prices histories on EIA (https://www.eia.gov/electricity/wholesale/#history). If you line up market timing and assume a requirement of about 6,600 BTU of gas required for each kWh of electricity. Then you would lose money for a fraction of production time without smart control.

[2] For example, see GE report on the implications of turbine operations on maintenance requirements. (https://www.ge.com/content/dam/gepower-pgdp/global/en_US/documents/technical/unused%20assets/hdgt-operating-maintenance-considerations-report.pdf)

[3] For example, see GE report on Kimberlite study about maintenance in Oil and Gas to prevent downtime: https://www.ge.com/digital/blog/study-digital-helps-lower-unplanned-downtime-oil-gas.

[4] For example, see International Data Corporation (IDC) report, which sites the Mining statistics: https://www.ge.com/digital/sites/default/files/IDC_OT_Final_whitepaper_249120.pdf

[5] Various organizations, frameworks, and individuals have tried to redefine or replace the Purdue Model over the years. Additional models are always great to consider but the Purdue Model, in its original form, was always meant to be flexible for future unforeseeable additions, such as IIoT. The Purdue Model is not used here as an example of the only way of modeling an environment but instead as a common reference model that is common to the lexicon of many security practitioners.