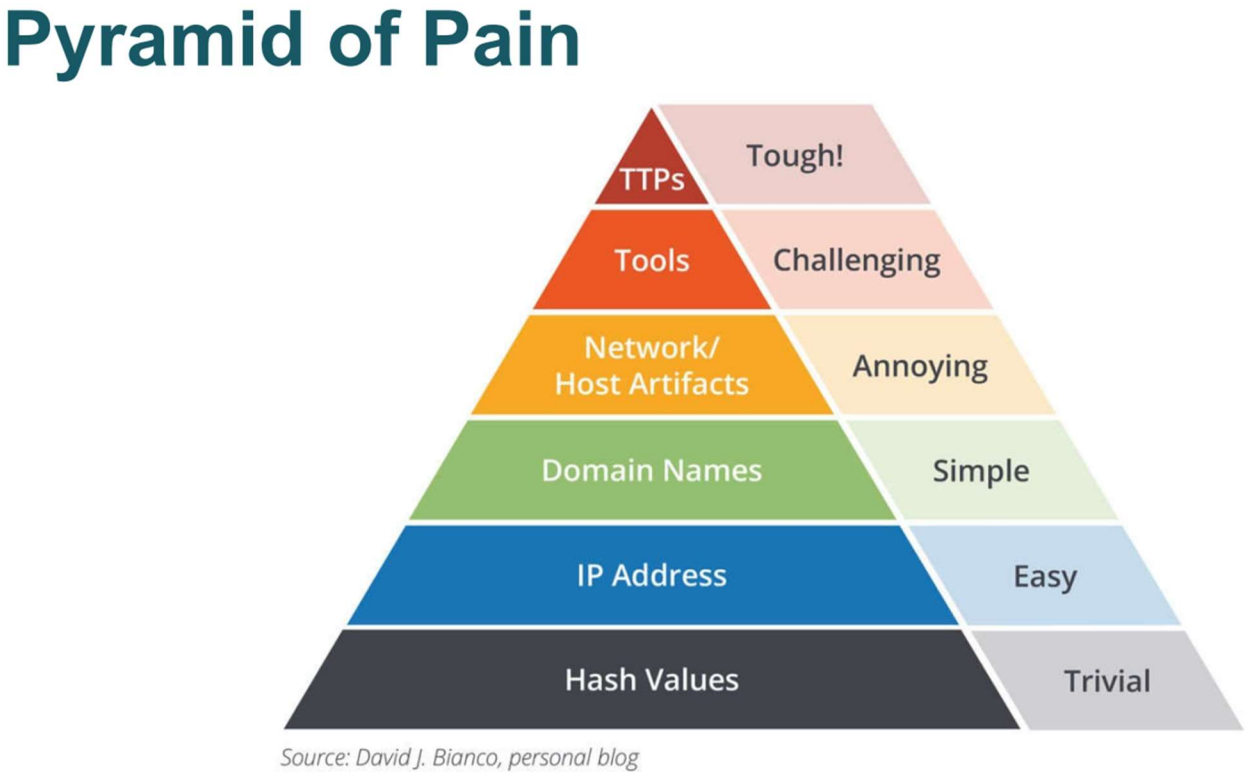
GRANTEK

Cybersecurity Risk Management from Grantek:
Using ICS ATT&CK Strategies

Background

Risk assessments and mitigation are commonplace activities in the manufacturing environment, but as the number and type of cyberattacks increases in all industries, it is necessary to take a practical, targeted approach to cybersecurity risk management of industrial control systems (ICS). Grantek, as a leading systems integrator and business consultant, offers ICS cybersecurity risk assessments based on the MITRE ICS ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). The ICS ATT&CK framework presents the information in matrices arranged by attack stages, from initial system access to data theft or machine control. The tactics, techniques, and procedures (TTPs) describe patterns of activities associated with a specific threat actor or group of threat actors. By leveraging the ATT&CK framework within a risk assessment process, Grantek is able to identify risks and associate them to TTPs that adversaries are actually using today. This, in turn, helps identify the specific changes which can be made to the systems and network environment to disrupt those attacks and significantly reduce the OT environment's risk level.



Source: David J. Bianco, personal blog

The MITRE Corporation's federally-funded cybersecurity R&D center helps to provide the nation's business infrastructure with effective and practical cybersecurity architectures and solutions. The ICS ATT&CK matrix provides a knowledge base of adversary actions and focuses on adversaries whose goal is disrupting ICS. This open-sourced/community driven knowledge base is accessible at: https://collaborate.mitre.org/attackics/index.php/Main_Page

In the ICS ATT&CK matrix, disruptive tactics are mapped against mitigation techniques to provide practical actions manufacturers can take to help prevent each type of threat. Information is also provided about adversary groups. Grantek's ICS Cybersecurity Specialists know how to use the ATT&CK framework to create a roadmap prioritizing mitigating the largest risks to an organizations ICS environment.

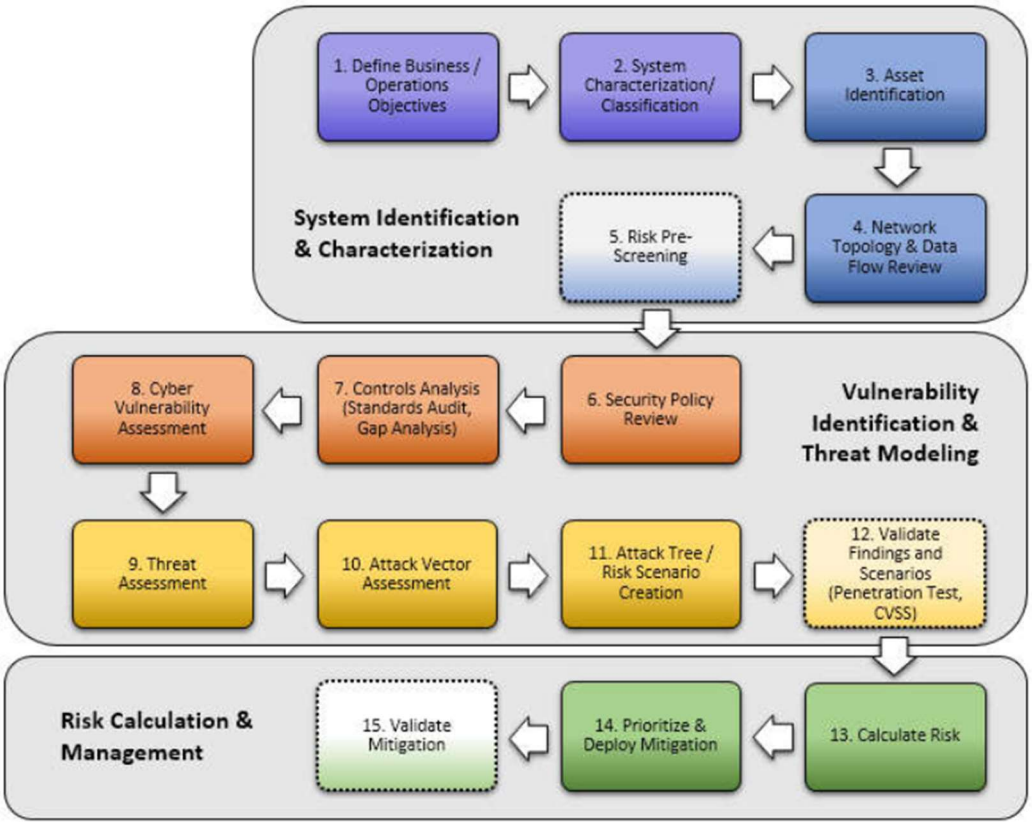
Applying ATT&CK to Risk Management

Applying ICS ATT&CK to risk management involves identifying cybersecurity risks, then determining the potential impact and likelihood of risk occurrence, and then determining the best way to deal with each risk with the resources available. Assessing this information helps manufacturers deploy the most efficient, cost-effective risk control and mitigation strategy and controls in a targeted way to reduce the most likely/highest impact cybersecurity risks first.

In the typical risk assessment methodology, an estimate of risk probability is required. Unfortunately, there is no simple but consistently accurate way to measure probability (likelihood of risk occurrence). Rather than relying on elaborate mathematical models or falling back on a guesstimate approach, ICS ATT&CK provides a more practical approach. Some aspects of this include looking at localized data relevant to the specific environment. Risk assessment is more about prioritization than probability, so it is important to evaluate local attack vectors. It is also important to use facts and measurable data applicable to the facility's configuration and assets to estimate probability rather than guessing or generalizing. Understanding the impact of a risk occurrence is more critical than its probability.

Because of our extensive experience with integrating manufacturing systems, Grantek is uniquely positioned to help manufacturers conduct ICS cybersecurity risk assessments and mitigation planning. However, for a risk assessment to be effective, it is important for manufacturers to have a complete understanding of the assets involved in their industrial control systems and the network topology in manufacturing areas. Legacy equipment, security patches applied or lacking, and connectivity to business systems with more threat exposure must all be considered when evaluating cybersecurity risk.

Typical steps involved with threat modeling and risk management are shown in the following diagram. Grantek's ICS Cybersecurity Specialists can help companies map their operations into a process like that shown below in order to conduct an effective and accurate risk assessment.



Practical Approaches to Preventing Cyberattack

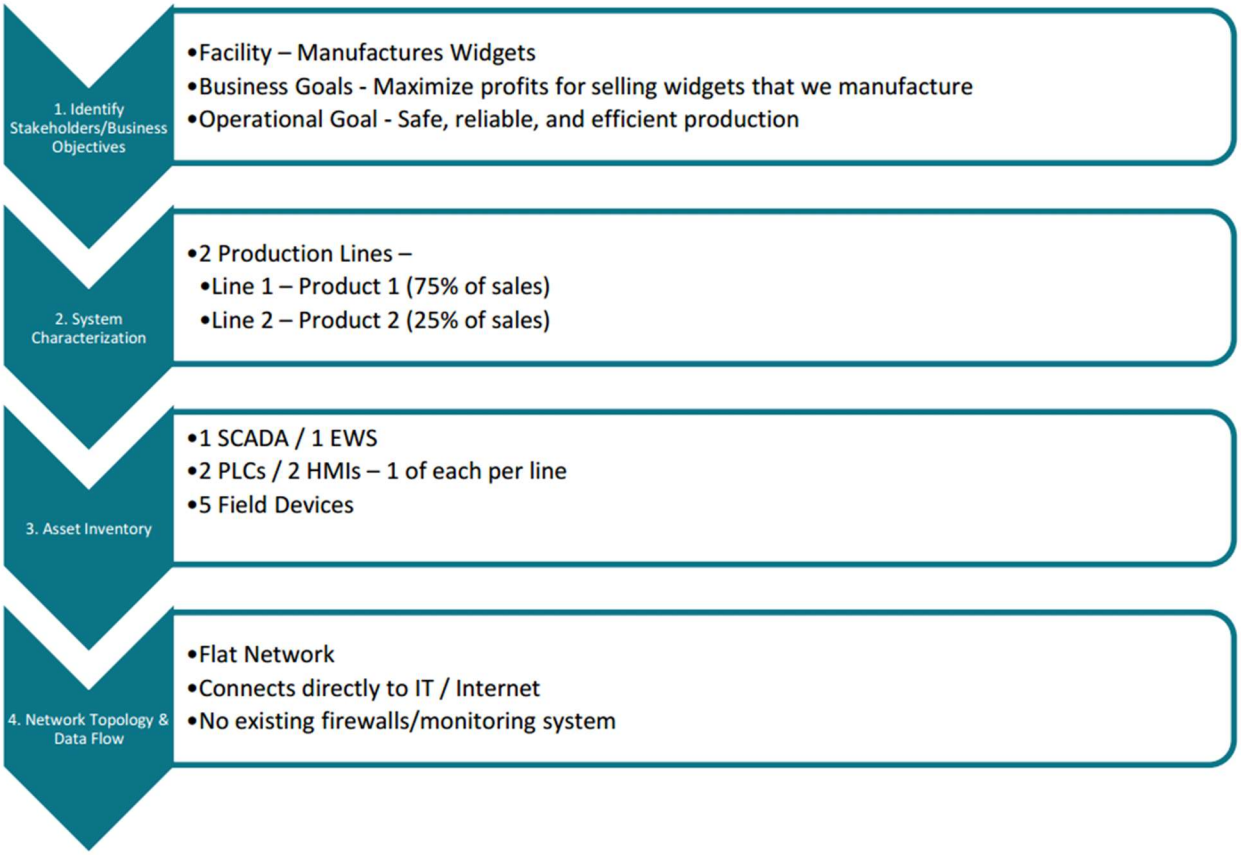
The use cases of the ICS ATT&CK model assume that a breach has already occurred, but Grantek's approach is to help plan and perform the preventive maintenance needed to fortify an enterprise's perimeter and internal network to help prevent an attack. Grantek can assist enterprises that lack the internal resources to perform this level of proactive cybersecurity risk assessment and preventive maintenance. In the chart presented above, Grantek's risk assessment services would typically be involved in steps 1 through 13 for a client, and can also assist with prioritization, deployment, and validation of the risk mitigation/corrective actions to be taken (steps 14 and 15). Grantek's broad manufacturing industry experience allows us to assist with prioritizing risk mitigation by identifying the biggest risks and addressing them first, then proceeding to the lesser risks. Proactive maintenance is always less costly than reacting after the fact, when time is of the essence and additional action may be needed to undo the damage caused by an intrusion.

Risk assessment typically consists or three phases:

Phase 1 – Gathering Information

Grantek consultants evaluate the manufacturing ICS system assets, links to networks outside of manufacturing, software/firmware installed on each workstation, controller, or other equipment, and user permissions, with consideration for other factors such as corporate expansion plans or equipment upgrades.

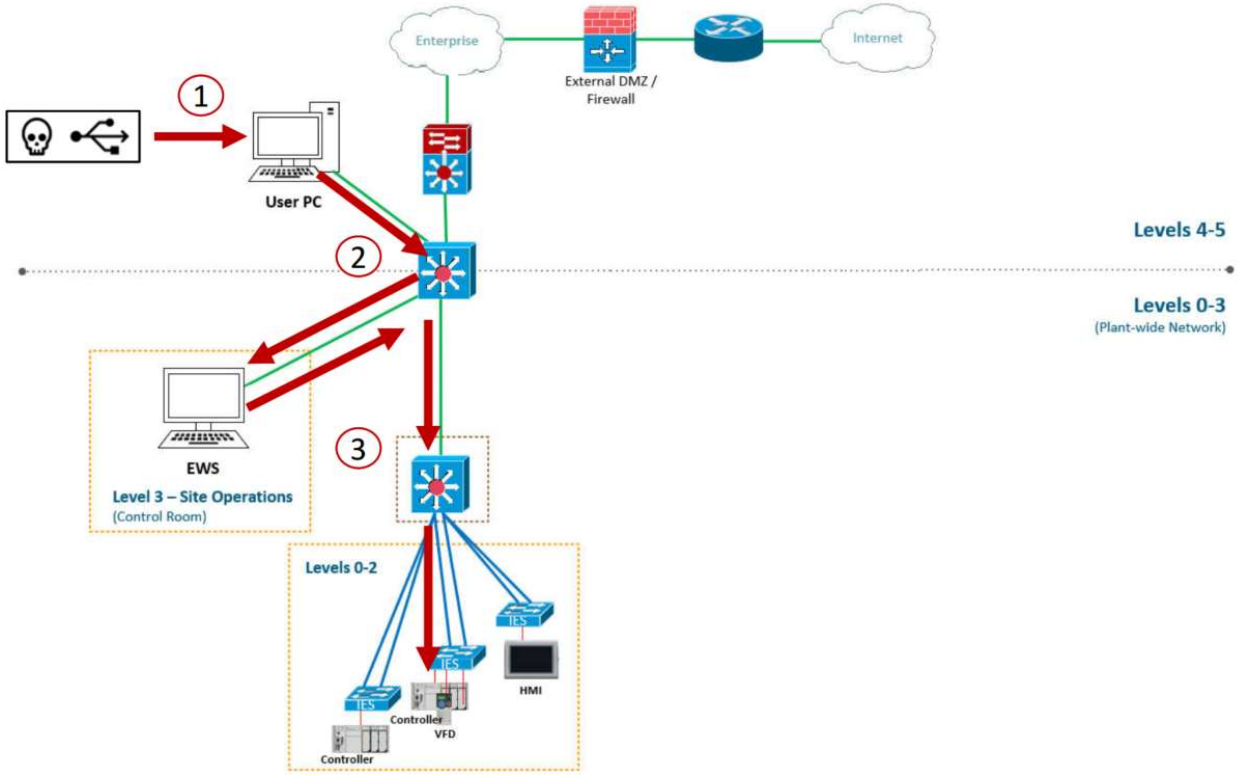
The following is an example presenting simplified findings of Phase 1.



Phase 2 – Create an attack tree example using ICS ATT&CK framework

The risks for each piece of equipment are defined and appropriate mitigation techniques identified and prioritized. For example, one attack tree may be a malicious USB connected at the Enterprise Network. Based on the flat network topology, the USB installs malware with the intent of gaining remote access to an Engineering Workstation (EWS). Once remote access is gained to the EWS, the adversary is able to leverage the ICS Software already installed and impair the facility's process.

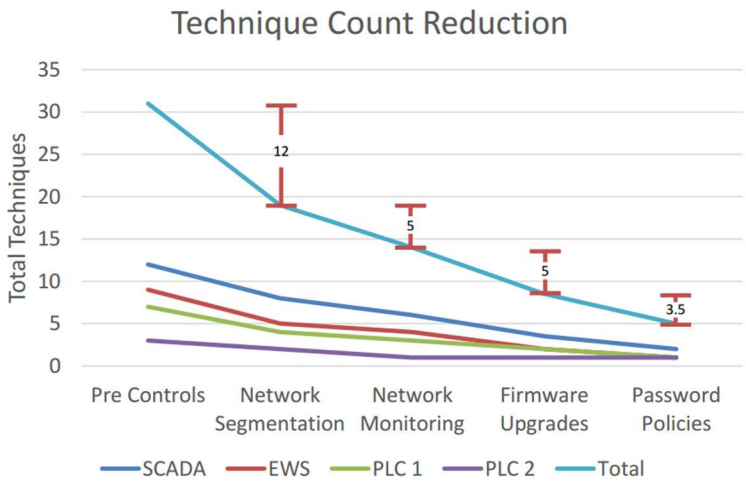
Example of Poor Network Topology



Phase 3 – Plan creation

Based on the findings of Phase 1 & 2, Grantek's ICS Cybersecurity Specialists are able to calculate asset risk and identify the cybersecurity gaps that may result in unwanted adversarial activity. Using this information, we are able to create roadmaps prioritizing these risks while also visually modeling risk mitigation once these risk mitigation activities have been performed.

1. Network Segmentation
2. Network Monitoring
3. Firmware Upgrades
4. Password Policies



Realizing Efficiencies

Because of our extensive experience helping customers with expansion of manufacturing capability/capacity, Grantek is uniquely positioned to help our customers implement security enhancements in conjunction with other activities requiring planned system downtime. This minimizes the impact on production and of course is preferable to an unplanned shutdown caused by a cyberattack.

Grantek understands that updating legacy equipment critical to production must be done efficiently and with careful planning. By incorporating security enhancements at the same time as system design changes, the security aspects of the system can be validated along with the rest of the system. We can also help ensure that any system expansions or improvements are planned and designed with cyberattack prevention in mind.

When it is time for system acceptance tests/functional acceptance testing (SAT/FAT), Grantek can help ensure that the test procedures include steps for risk management, such as testing user permissions and ensuring the latest firmware is installed on each piece of equipment in the line.

Enterprise-Level Considerations

Most security breaches are the result of intrusions or malicious attacks on the corporate side of the enterprise. In the past, networked manufacturing systems and equipment were separate from the rest of the enterprise and the outside world, and only communicated with each other. But in recent years, with the advent of Manufacturing Execution System (MES) and Overall Equipment Effectiveness (OEE) implementations, there is greater connectivity between the enterprise network and the manufacturing network. Though this improves efficiency and allows for better planning, it also allows more opportunity for intrusions, malware, and successful phishing attacks, and allows malware to spread to the production floor with potentially catastrophic results. Grantek can assist with separating external and

internal systems using a network demilitarized zone (DMZ) to effectively isolate vital production systems from intrusion.

The rapid adoption of the Industrial Internet of Things (IIoT) also has the potential to allow intrusion, as more and more devices are networked, often with inconsistent implementation lacking enough security measures. As the IIoT is increasingly adopted, it may increase the vulnerability of the control system network if robust security practices are not rigorously followed. Cloud-based tools and systems also pose new risks that increase the attack surface.

When Grantek performs a risk assessment and mitigation plan using the ATT&CK model, we classify system assets based on criticality, not only from a manufacturing process perspective, but also from the perspectives of potential environmental, safety, and regulatory impact that could result from a security breach. The risk assessment/mitigation activities can be bundled with other Grantek services to take advantage of planned facility downtime.

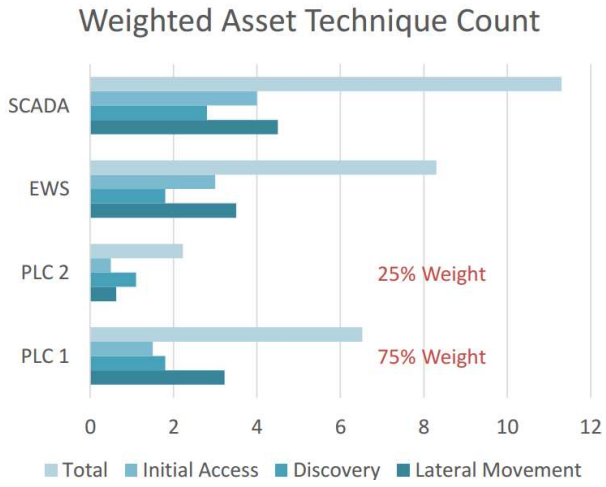
Our expertise in migrating legacy PLC systems, virtualizing servers, changing control panels and updating HMI systems allows Grantek to not only identify potential cybersecurity risks but also to efficiently mitigate them by upgrading equipment and accompanying firmware. Grantek knows how to design the digitization platform while ensuring system security.

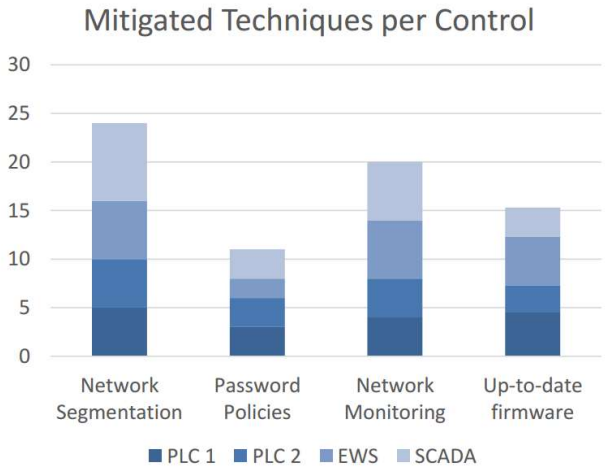
The ICS ATT&CK model is not a standard but provides a framework of known activities attempted by cybersecurity adversaries. It defines how adversaries have successfully attacked ICS and provides the mitigation steps to take for each type of known attack. Grantek then lines up the mitigations with the standards applicable to each area in order to provide an industry-compliant mitigation. Our implementations closely follow ISA-99 and IEC 62433.

Technology Experience

Grantek is a system integrator company, capable of providing the full range of technical services needed to enhance cybersecurity in manufacturing. Our knowledge and experience working with legacy and contemporary manufacturing control systems gives us practical experience in risk identification. Our cybersecurity risk assessment is built on the ICS ATT&CK framework and benefits from Grantek's practical experience as a systems integrator when it comes to security risk mitigation in industrial control systems.

Phase 3 – Prioritization





Grantek's role in helping our customers achieve and maintain a high level of cybersecurity typically starts by inventorying the manufacturing assets and assessing their vulnerabilities. Our experience as system integrators enables our cybersecurity risk assessment consultants to consider the overall goals of the enterprise, the manufacturing assets, systems already in place, and links from IT networks to ICS networks that create potential vulnerability. We can provide risk assessment as a stand-alone activity or as part of system buildout/expansion or equipment upgrade. Efficiencies are achieved by performing security enhancements concurrently with other planned activities. And of course, it is always preferable from the corporate perspective to improve ICS cybersecurity before an adverse event affecting production occurs, rather than being forced to deal with an intrusion and its consequences.

If your company is unsure of how to plan for attack prevention or is concerned about the cost of protecting operations, we can develop a plan to suit the company's needs. Grantek's cybersecurity risk management services are available to manufacturers aware of cybersecurity threats and concerned about bad actors harming operations or the company reputation. We can work to provide a solution that can be integrated with other activities in the areas of Smart Manufacturing, digital transformation, Pharma 4.0 or Industry 4.0.

Please contact Grantek to learn more about how our cybersecurity risk assessment and mitigation services can provide actionable solutions for mitigating ICS cybersecurity risks. For further information on Grantek's unique approach to implementation of the ICS ATT&CK framework, please view our webinar: https://youtu.be/pPUvjQWPFIg. If you or your staff would like more information about Grantek's cybersecurity capabilities, please email info@grantek.com.

For 40 years, top manufacturers in Food & Beverage, CPG and Pharmaceuticals have called upon Grantek to solve their most complex business and manufacturing challenges. Grantek automates Pharmaceutical and Food & Beverage manufacturing operations, including integration with business systems for seamless solutions. Grantek helps customers meet the stringent requirements and challenges of the 4th Industrial Revolution. Grantek's team of professionals located in 17 offices across the globe deliver solutions to complex problems in Smart Manufacturing, Industrial Networking, Automation and Industrial Safety. Call 1.866.936.9509 or email info@grantek.com to learn more.