WAYS TO KEEP AUTOMATION AND CONTROL SYSTEMS SECURE

LAFAYETTE ENGINEERING INC.

"Cybersecurity is much more than a matter of IT."

- Stephan Nappo

In decades prior to the 21st century, cybersecurity just wasn't an issue because the cyber world simply did not exist. And the cyberworld is glorious — allowing enterprise engineers, operators, and IT workers to run their operations from anywhere in mere seconds. The global networks allow for greater precision, flexibility, and control of automations and systems — in ways we never thought possible.

But with this great privilege comes great responsibility. Since the internet became a global commercial network in the 90s, cybersecurity has been an ever-present issue.

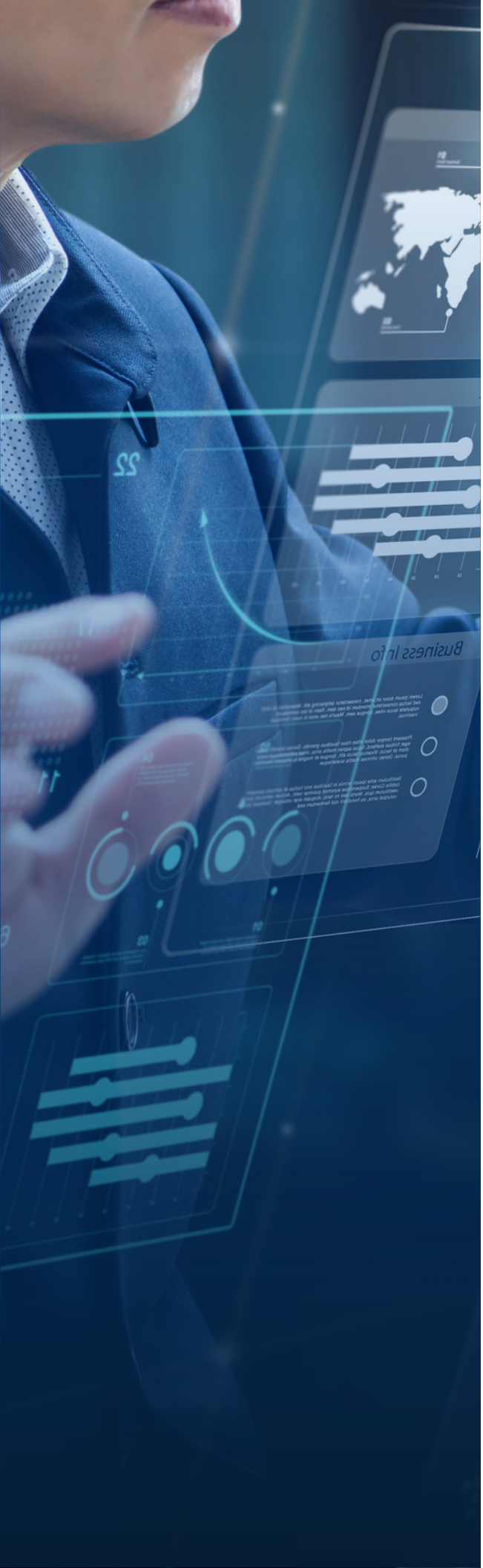
And though this has opened the door for plentiful opportunities to work with other individuals and networks around the world, it has also opened another door to outside threats. With access to control systems via the network, cybersecurity issues have significantly increased over the last two decades. Thus, engineers and automation specialists must do more to stay on top of the game and keep automation and control systems secure.

Is there hope for a better, more secure solution so facilities can serve this fast-paced environment?

Absolutely! You shouldn't have to feel overwhelmed by all the updated regulations.

In this guide, we discuss 3 strategies that will help you keep your automation and control systems more secure.

Let's dive in!



1 RECOGNIZE THE RISKS

Control systems are vulnerable to a variety of cyber security issues. PC-based systems are more vulnerable, and thus especially benefit from pre-emptive risk assessment. One way to tackle these vulnerabilities in control systems is through network segmentation, a process in which your network is divided up into multiple zones with separate security protocols for each zone. By doing so, your organization's devices, servers, and applications are isolated from the rest of the network. Network segmentation is a "patchwork" approach, though, and there are other ways to head off your control systems security risks.

Human Machine Interface (HMI) systems such as dashboards or screens to control and monitor machinery are also one of the most targeted aspects of an industrial control system. The good news is that you can take steps to secure your HMI, such as an "onion" approach. For example, consider creating layers of security — considering the physical environment, the network, the host and operating system, and the HMI itself.

The important thing is to recognize which areas of your facility are most vulnerable to hacking, and what the fallout could mean for each area. For example, if a system is hacked, and sensors are no longer functioning, boxes will not be directed into the correct lane —causing potential pile-ups, damaged packages, and hours or days of lost productivity.

2 SECURE ARCHITECTURE

Although no system is ever bulletproof, an ideal architecture is built to be flexible despite the continuously evolving cyber threats. Developing and maintaining the integrity of your security architecture is not a one-time process. As businesses grow and change, the continually changing environment will require you to closely monitor your security architecture, and modify when necessary.

You can't protect anything unless you know what you have. Cybersecurity architecture is the manner in which various components of your control system are organized, synced, and integrated. It is a set of people, processes, and tools that work together to protect your company's assets. Facilities evolve over time, and as a result, a system's architecture can get complicated. *This is hugely critical to avoiding disaster.*

- *Start with understanding your operating system and the security already in place.*
- *Be knowledgeable about any and all software you implement.*
- *Identify where all components are, and who has physical as well as remote access.*
- *Determine which isolated systems rely on products from other isolated systems to operate.*
- *Document what servers, controllers, sensors, etc. your system uses and who can digitally access them.*

3 DEVELOP AN ACTION PLAN

Once you've identified the risks, it's time to start with the strategies. It's important to create actual documents for the plans that you create so that everyone involved can agree and follow. Plans should be shared with employees on how to protect digital assets(maybe resources) from cybersecurity situations, including a recovery plan in case of emergencies.

Consider developing and documenting these security plans for your facility's control system:

- A Risk Management Plan
- A plan to fix current issues
- An Operational Technology (OT) Security Policy
- A plan to follow and enforce the OT Security Policy
- A Disaster Recovery Plan

When creating these plans, be sure to note how often your system audit is updated, as well as what risks are minor and can be anticipated and ignored. Work closely with your I.T. team to develop and improve online and offline security for all areas of your ICS.

NO SYSTEM IS 100% ERROR-PROOF...

But minimizing risk and preparing for the worst are just smart business decisions for industrial facilities. You must ensure the equipment that runs your facility and the data that powers it all is protected from outside threats.

As we become more aware of risks, and as technology continues to evolve, online security issues will also continue to grow and become more complex. The best way to protect your assets is to stay ahead of the curve, be proactive, and implement a firm but flexible strategy.

Helping manufacturing companies simplify their automation system through design and installation is what we do — all day, every day.

If you need help creating security plans for your facility, our engineering experts can help. Give us a call today at (844) 845 - 7580.

CONTACT AN EXPERT

LaFayette
ENGINEERING, INC.

We help distributors design and install conveyor systems programmed to increase productivity and move products more efficiently.