Industrial IoT Markets & Security

# When Security Standards Aren't a Standard

*Weaknesses in Cyber and Network Security Standards*

**Garrod Massey**

**- Operations, UCEC Smart -**

A Publication of

UCEC SMART™

# Cybersecurity in the Industrial Workforce

*Cyber & Network Security Weaknesses*

Spending the last 11 years in the industrial workforce providing electromechanical safety certifications for industrial control systems, I have been exposed to many different projects in various industries. These industries are vast and include Oil & Gas, Utilities, Renewables, Food & Beverage, Mining, Pharmaceutical and many more. Although they produce different outcomes, many of these industries employ the same types of people. Skill sets range from purchasing/procurement, accounting, design/drafting, engineering, programming, install/startup, management and so forth. The common weakness in all of the aforementioned industries is cyber and network security standards.

# Beyond Component-Level Certification

In my tenure, I have provided hundreds of UL (Underwriters Laboratories) certifications on industrial control panels that are being installed all over the globe. These systems require certain overall certifications dependent on the environments they are being installed in. Panels installed in non-hazardous locations mostly require a standard UL-508A (NITW) certification, while other systems installed in hazardous or potentially explosive environments require UL-698A (NRBX) or UL-NNNY. Though daunting at times, the process of certifying one of these cabinets goes way beyond component level certification. We have to make sure all necessary parts will work as intended, while playing well with the vast array of other electrical and mechanical parts within the cabinet. To do this, we have to take a deep dive into each and every part on the bill of materials. Firstly, each part will require a UL certification from the original manufacturer. There are two type of marks from UL. They have " UL LISTED" and "UL RECOGNIZED"[1].

Either of the two marks mean the component has had some level of certification from Underwriters Laboratories. Now, these marks don't automatically mean we can use the components in our intended applications. We must also explore the specific UL file number of the component in question. This number and associated documentation allow us to verify the certification is real and valid at the time of use and is unique to only the manufacturer of the component in question. Within the UL file they show us yet another component identifier called a category control number. The category control number is what links this specific device to other manufacturers similar components.

Now that we have the category control number we can check to see if the component can be used in our cabinet. To do this we must visit UL's website where they host a document called "Supplement SA". In this document we can do a search of the category control number. Each category has a notes section, which if empty means we can use the part with no issue, however most of the time there is a specific note stating how the component has to be used or stating we cannot use it at all unless we pay UL to certify our company to do so. This is called procedure described. All of this just to see if we can use one component!

You might be asking, "Where does network security and integrity come in?" The answer: Mostly at the component level.

Now that we know the parts are usable, we have to install them per the manufacturer's instructions, while maintaining all of the air and wire bend ratio clearance specifications within the UL-508A book. In the installation and wire phase, we have to use UL traceable wire, NIST certified and yearly calibrated torque and measurement tools, as well as all applicable NEC, ANSI/NFPA70 electrical safety requirements. When all of this is said and done, UL now requires us to place proper equipment safety and convenience markings in the cabinet, notifying operators of voltage, current, phase, frequency, fuse replacement charts, electrical fitting penetration requirements and many more. Each application will require standard markings and panel specific markings.

At this point, after inspection and powering of the equipment, we can give our panel a UL certification. All of these steps allow an industrial control panel to pass a electrical inspection at the final install site, thus allowing the end user to run processes from emergency stops to critical infrastructure. You might be asking, where does network security and integrity come in?

The answer: Mostly at the component level. Each one of these network accessible components is generally loaded with some level of software programmable security built in, but is this good enough?

As consumers we tend to purchase items based on how safe the datasheets, commercials or advertisements make them seem. This feel good stage is  enough to get most designers and engineers interested in these products without first architecting the systems security structure. If the components says it has Virtual Private Network (VPN) functionality or says it has AES 256 Encryption, that will drive most people to buy them regardless of how they will actually be used or configured. It is generally implied that these safety measures are implemented as soon as the device is plugged in, leaving your home or business “safe”.

# Lack of Security Knowledge

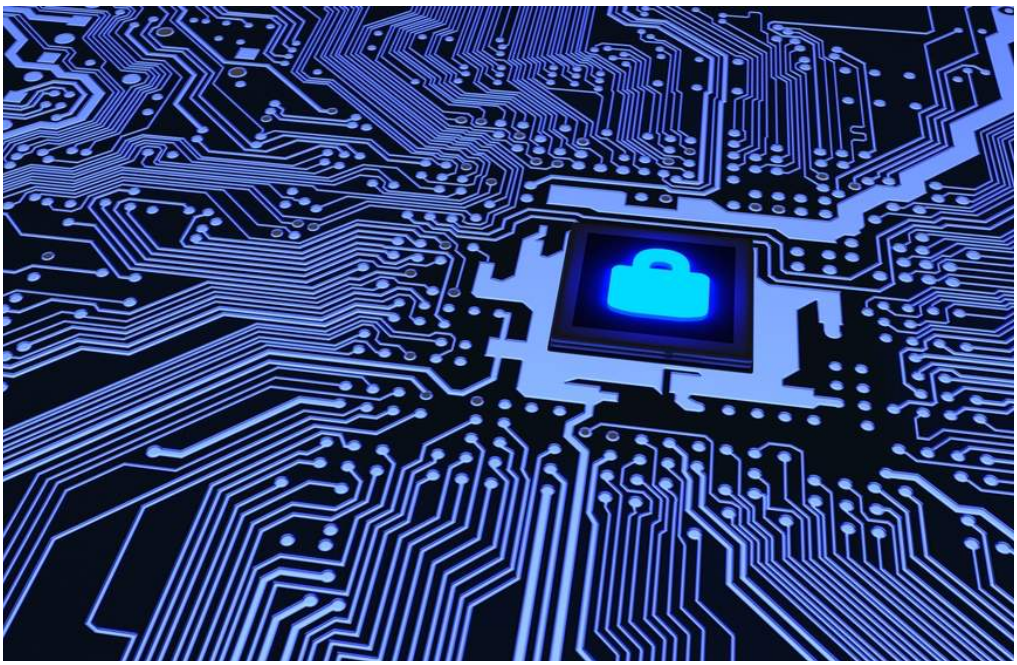
While reading or watching the news we become outraged when hearing of data breaches and security hiccups. Although consumers get angry at these headlines, they too are often lacking basic security in their own networks. Paul Wagenseil explains, “Eighty-two percent of 2,205 people surveyed said they had never changed their router's default administrative password. Similarly, 82 percent had never changed the default network name, 86 percent had never updated the router's firmware, 70 percent had never checked to see if any unknown devices were on their networks and 69 percent had never even changed the default Wi-Fi access password. More than half the people surveyed — 51 percent — said they had never done any of these things, and 48 percent didn't understand why they would even need to.”

He goes onto say, “ When asked why they hadn't taken these basic steps, 34 percent of the respondents said they didn't know how, six percent said they couldn't understand the instructions and three percent said the software was confusing. And these were the 52 percent of respondents who at least knew they should do these things[2]. Though this example isn’t industrial specific, it definitely carries over. The problem here is that most people are under-educated in modern electronics and cyber security. If you have never taken a course, chances are you will not understand what the user guides are asking you to do, so most of the time these security measures will be ignored.

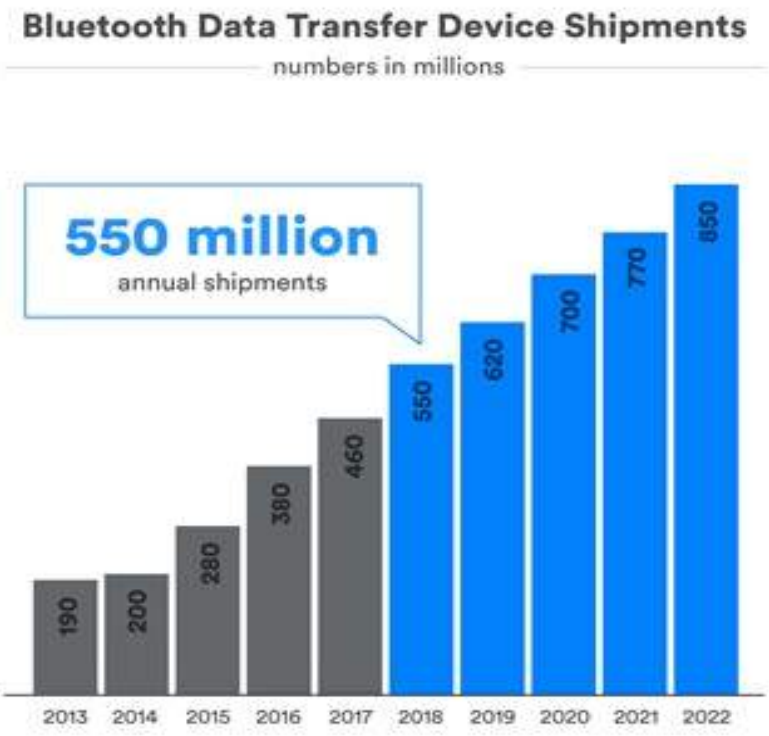
82% of consumers never change their router’s default administrative password nor changed their default network name.

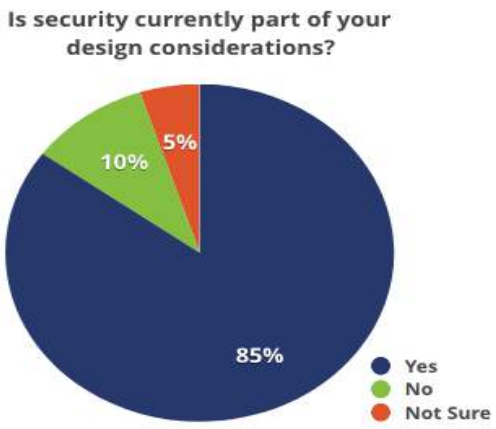
What needs to happen from the parts developer standpoint is simple. Build the device with a security at all levels mindset. Since these types of network devices are sold for consumer and industrial applications, there should be a forced level of security built into the software to make the end users take advantage of the built in security and giving people a clear explanation of what the importance of these items are. Paul goes onto say, “We can't completely blame the users for their ignorance, just as we can't expect every car owner to know how to change the oil or adjust the brakes. But at least most car owners know they should get a mechanic to do those things for them.

By contrast, ISPs and router makers have clearly not done enough to educate their customers on the basics of router security. Some newer routers don't expect their users to know all this -- they come with randomized administrative passwords or network names, or force you to change the default administrative password when you set a router up. Many mesh routers automatically update their own firmware, which is also good, though it won't do much to protect you if the administrative password is still the factory default[3].



In 2019, my company will begin forging into the IoT and IIoT space. These markets are dominated by low power consumption nodes talking via relatively new wireless protocols. Choosing the most well rounded product becomes challenging because there are so many players racing for their section of the market share; but to what cost? Lack of security through the entire stage of the embedded design is one of them. Many small companies have designed these nodes based on simple coding templates using arduino's or rasberrypi's. This can lead to huge physical and intellectual security breaches costing the consumer and developer lots of time and money. It would appear that these developers are thinking their devices won't get hacked or the security will happen further along down the chain. With a good amount of these devices using Bluetooth Low Energy (BLE) protocols, the issue becomes what grade of security they will be developed with. Due to price and time to market constraints, some of these nodes will make it to market with the standard BLE specification of 6 digit temporary keys (TK). This will allow fairly easy access via a brute-force attack due to the short range of options. With 850 million of these device planned to ship by 2022, there will be a lot of low hanging fruit for the black hat hackers[4].






In a recent survey of 252 developers, we find that “security was a part of the design considerations for 85% of the respondents and slightly less than 10% indicated that it was not. Of those who said security was not a part of current design criteria, the reasons range from not necessary, not a customer requirement, too much trouble and too expensive being almost equally weighted at slightly over 10% each. The predominant reason with over 50% justifying lack of attention to security in their design approach was that it was handled in another part of the system.[5]

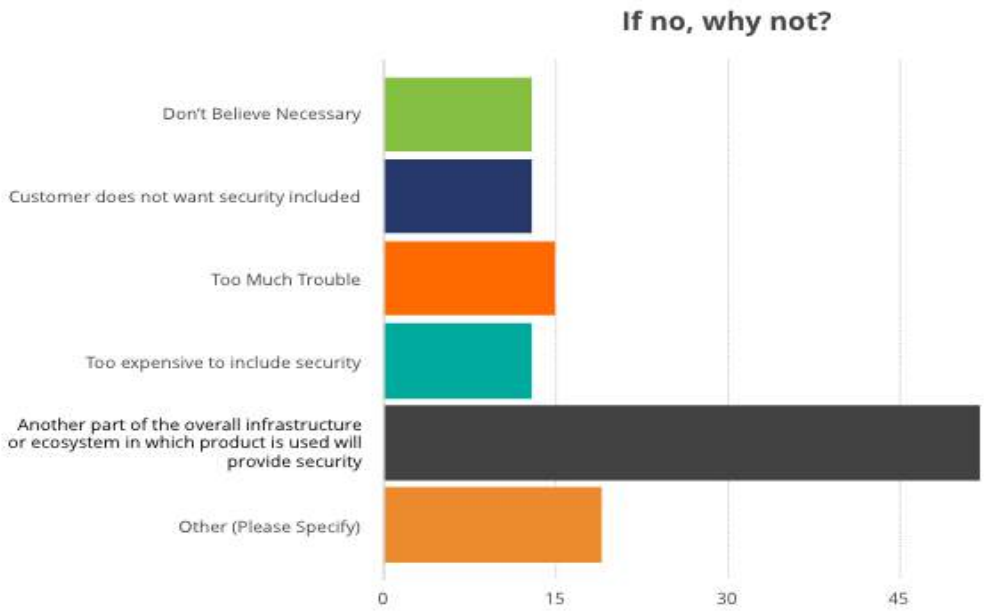
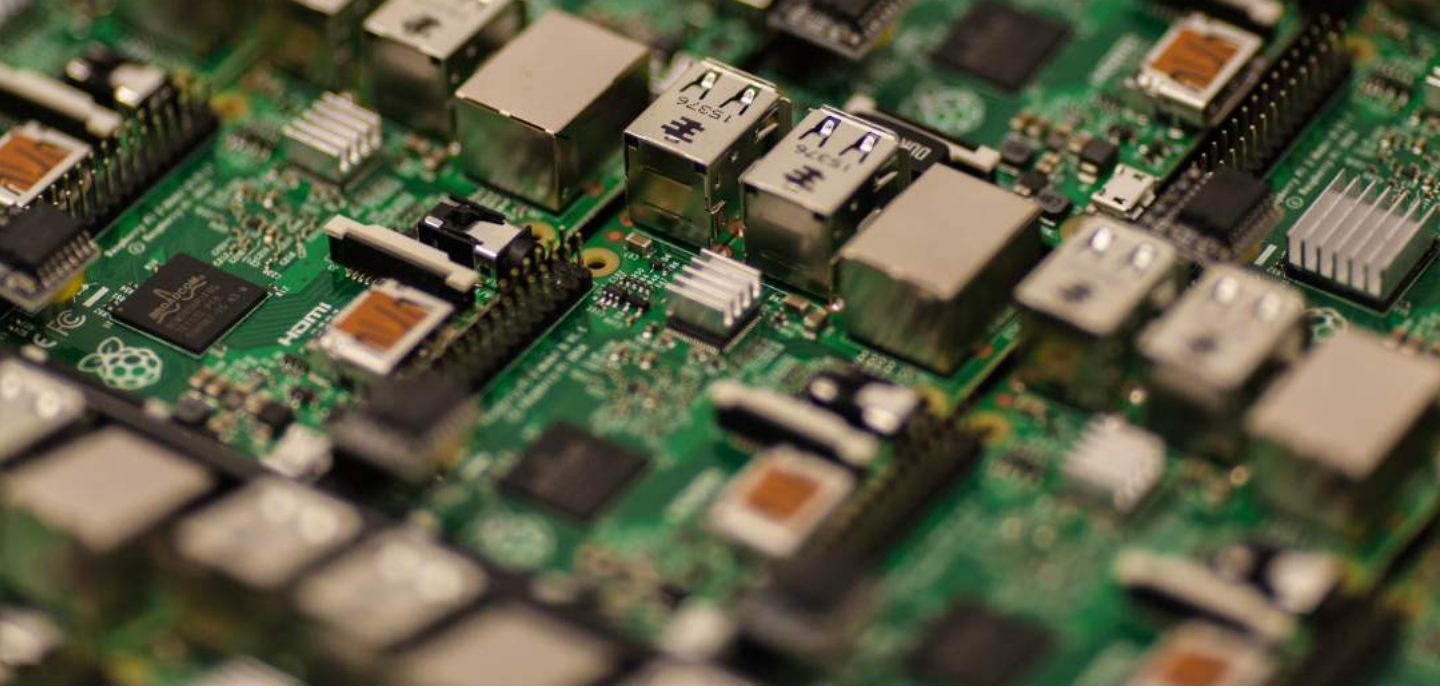



*Figure 3 Reasons to not consider security in current designs.*



# Safety Standards Aren't Standard

At the end of the day, we take electrical safety way more seriously than cyber safety. More consumers and businesses are affected by hacks and data breaches than electrical injuries by a long shot. "There were 1,640 nonfatal electrical injuries resulting in days away from work in 2016, one-third fewer than the 2015 number"[6], while "Hackers have exposed the personal information of 110 million Americans -- roughly half of the nation's adults -- in the last 12 months alone"[7]. This is equal to nearly 47% of American adults. Now, I'm not saying we are over thinking personal safety, we are just way under thinking cyber safety. At a minimum, we should have a couple of National Certified Test Agencies that implement mandatory safety standards at the component and system level, before any product can go to market. The integrators and manufacturers should carry responsibility for system integrity by making sure to follow all the rules and implement standards like the NIST AES 256 encryption protocols. These systems, when designed and paired with other parts like programmable logic controllers(PLC), industrial pc's(IPC), ethernet switches, firewalls, controllers and so on, should be given a full system stamp of approval, just like we do for industrial control panels via a UL listing. This would force the issue of security, thus leaving consumers and businesses to worry about their core.

In conclusion, I have been given a new light on cyber security. As a people we need to come together to reinforce the idea that change is going to happen no matter how much we push back, but it can be done safely and securely. With a new evolution of standards, we can insure that our future is safe and secure!

# Endnotes


1. UL Certitfciations: https://markshub.ul.com/
2. The One Router Setting Everyone Should Change (But No One Does): https://www.tomsguide.com/us/change-router-default-passwords,news-26975.html
3. The One Router Setting Everyone Should Change (But No One Does): https://www.tomsguide.com/us/change-router-default-passwords,news-26975.html
4. The Expansion of the Connected Device Market: https://blog.bluetooth.com/3-connected-device-segments
5. What Embedded and IoT Developers Think About IoT Security: A Look at Survey Data in 2017: https://trustedcomputinggroup.org/wp-content/uploads/What-Embedded-and-IoT-Developers-Think-About-IoT-Security_Survey-Report.pdf
6. Workplace Injury & Fatality Statistics: https://www.esfi.org/workplace-injury-and-fatality-statistics
7. Half of American adults hacked this year: https://money.cnn.com/2014/05/28/technology/security/hack-data-breach/


UCEC SMART™

www.UCECSmart.com