CYBERSECURITY, SAFETY AND RELIABILITY

Howard W Penrose, PhD, CMRP
MotorDoc® LLC
Lombard, IL 60148

Abstract: The charge forward of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) consistently leaves out concepts of ensuring the security of a company's critical control and computer systems. It is even more serious when some sales organizations attempt to sell their IoT ideas with recommendations to maintenance leadership of how to get around Information Technology (IT) departments and rules. Further, the lack of understanding of what systems could be considered cyber-related and undergo security checks and steps is significant. The impact of cyber-holes in the system include the loss of systems, damaged systems and potential safety hazards. However, the implementation of cybersecurity is not far-fetched from reliability programs that already exist and, especially with the rapid deployment of cyber-devices, a way of further justifying the application of such programs as Reliability Centered Maintenance (RCM). In this whitepaper we will focus on one of the items of Cyber-Physical Systems (CPS) called Trustworthiness.

INTRODUCTION

The implementation of cyber-information and cyber-physical systems (CIS and CPS), often referred to in marketing terms as IoT and IIoT, has the potential of improving overall operations, production, service, maintenance and living conditions with relatively low expense. IoT sensors and devices are critical to machine learning (sometimes referred to as artificial intelligence) as well as remote operation and monitoring. This has all led to significant amounts of data that is now referred to as 'Big Data,' which generally means: 'overwhelming for the average individual.' Whether it is the workplace or home, the ability to use cyber devices improves overall living and has the potential to manipulate surroundings at home and work.

However, any device that has IP and MAC addresses have the potential to be exploited deliberately or by accident unless appropriate steps are taken. If you were not aware, even devices such as energy monitoring, variable frequency drives, and safety devices have IP and MAC addresses, with the potential of creating a cyber-hole into your system if they are not set-up correctly, and most aren't. This is just one example of the hundreds of systems that you already have in-place that can allow access to your system. Couple this with vendors who either neglect to mention, let alone those who deliberately describe how to avoid, the implementation of security protocols, and you have a recipe for disaster.

But the technology was purchased by a known company. However, there are no third-party or standard methods for ensuring the trustworthiness of an IoT or IIoT device. Even with larger companies, the devices delivered are not always as secure as you would expect. With some companies, devices are produced that deliberately deliver information to hostile organizations or governments that sell or share the information. While rarely making the front page news, most of the time just being mentioned. It is serious enough that hostile 'smart-bulbs' that would share your WiFi logins and passwords to hackers associated with the manufacturer of the bulbs are still in use!

While many are calling for a certification program or processes for ensuring the trustworthiness of CPI and CPS, and some efforts are underway, IoT and IIoT certification organizations are not being seen as a priority at this time.

IMPACT ON SAFETY

There are many stories, including by companies that you would think wouldn't be targeted, outlining significant impacts as the direct effect of hacks into weakly secured systems. These can be as simple as changing or removing safeties, 'spoofing' information and feedback while manipulating devices, disabling response systems, harmful operation and denial of service. What would the impact be on one of your systems if a critical compressor was repeatedly turned on and off? If a pressure vessel near personnel was overpressurized to rupture?

CHALLENGES

There are a great many systems and conditions that present challenges to the ability to control cybersecurity issues and the trustworthiness of cyber systems. These include:

- Legacy systems – earlier systems that have no security or compromised security;
- Education – of maintenance and reliability professionals;
- Vendor updates and upgrades – either not being performed to upgrade security or generating holes in secure systems;
- No certification program – for ensuring trustworthiness of devices;
- No common practices or processes for checking and ensuring device trustworthiness;
- Human elements – the 'go around' of secure systems;
- The ability of hostile elements to exploit weak systems through detection of those systems with specialized search engines (ie: Shodan.io) and software; and,
- A recent survey of IoT and IIoT articles identified less than 1% even discussed cybersecurity and exploit issues.

In addition to the above, one of the more significant issues is that small to medium companies have received little to no support or education. This is interesting as these are the companies that both are the ones being targeted and have the least resources to protect and educate. The result has been that many of the successful attacks on larger organizations are initiated through third party vendors through exploit emails and other attacks that require a higher degree of sophistication to protect against.

While half of cyber-attacks are by outsiders, it is also important to understand that roughly 25% are instigated by disgruntled employees or other 'insiders.' The motivation behind attacks are strictly opportunistic (easy to hack) at 49%, dissatisfaction with employer 15%, and industrial espionage/financial crime/terrorism/data theft running 23%. In effect, less than 1 out of 4 attacks are financially inspired, which means that the potential risk exists across the spectrum.

INDUSTRY MAINTENANCE DEVELOPMENT PRACTICE

During a literature review, several academic articles discussed a 'new concept' of the FMEVA, or Failure Modes, Effects and Vulnerability Analysis, for CIS/CPS. However, when reviewed, it appears to be more an attempt at the appearance of something new versus the true basic FMEA utilized in physical asset management that it really is.

It appears that some key items related to systems undergoing RCM are outright ignored. In effect, the impact of cyber vulnerabilities is supposed to be part of the RCM process.

The general discussion and existing frameworks that have been developed to guide organizations, in particular public organizations, in cybersecurity have been quite complicated and daunting. This is where the existing process surrounding RCM comes into play. It is important to remember that not all failures can or should be prevented. Risk management is good policy.

The steps necessary to evaluating physical assets:

- Asset Census
- Criticality Analysis
- RCM Process
- Maintenance Effectiveness Review

The criticality analysis involves determining the level of analysis, or if an analysis will be performed, based upon:

- Impacts on personal safety
- Regulatory or environmental impacts
- Mission or operations
- All others – cost impact or special

The systems determined critical based upon a company's criteria from above are then applied to the seven steps of RCM.

1. Function: what are the functions and associated desired standards of performance of the asset in its operating context?
2. Functional Failures: in what ways can it fail to fulfill its function? This would include the potential impacts of cyber issues, easily determined if the system has an IP or MAC address.
3. Failure Modes: what causes each functional failure? Including cyber issues.
4. Failure Effects: what happens when the failures occur? Including compromising other systems.

5. Failure Consequences: in what way does each failure matter?
6. Tasks and Intervals: what should be done to predict or prevent each failure?
7. Default Actions: what should be done if a suitable proactive task cannot be found? Can the system be made more resilient?

The FMEA itself follows several basic steps:

1. List the function being evaluated
2. Define the functional failure
3. Determine failure modes
4. Failure effects at:
    a. Local
    b. Subsystem
    c. System

While the purpose of this paper is not to develop an RCM or FMEA process, it is primarily to bring the reader to the realization that the cyber portion of the systems that are being applied and that have access to an intra or internet, need to be considered when developing a maintenance program. Tools exist to ensure that the system is either developed to be resilient, secure or both.

CONCLUSION

Vulnerabilities exist in every organization that make that organization susceptible to cyberattacks. The application of RCM must consider the CIS and CPS impacts on these systems, otherwise the RCM process is not being fully utilized. Otherwise, the potential for damage to the system and the potential for personnel safety issues become significant.

Reliability and maintenance professionals working with IT departments can improve the reliability and resilience of systems significantly. Just because a company does not appear to be a potential target, it doesn't mean that they will not be attacked. It becomes important to ensure that RCM processes are fully exploited before a company or organization is tested by a malicious entity.

ABOUT THE AUTHOR

Howard W Penrose, Ph.D., CMRP, is the president of MotorDoc® LLC, vice president of MotorSight Corp, Editor-in-Chief of the IEEE DEIS Web, and Treasurer of SMRP as well as serving as the Chair of the Government Affairs Committee of SMRP. In addition to his professional duties, Dr. Penrose has been representing maintenance and reliability professionals in relation to cybersecurity and infrastructure with policy makers and NIST. Dr. Penrose can be contacted by email at hpenrose@motordoc.com.