CALLIBRATION CYBERSECURITY RISKS

James McGlone
Kenexis
3366 Riverside Drive, Suite 200
Upper Arlington, Ohio 43221 USA
Telephone: (614) 643-2473
james.mcglone@kenexis.com

Abstract: Hardly a day goes by anymore without hearing about a cyber security event in the news. In this paper/session, we will analyze the risk associated with smart devices, calibration, and maintenance that could compromise the cyber security status of operations and possibly our entire companies.

As a nuclear power plant operator and electronic technician, we never considered the security risk of having an instrument calibrated by a third party. Today however, things have changed significantly and it is common to find microprocessors in virtually everything including the instruments we are using in our plants. The microprocessor has made significant impacts in performance and communications and consequently might be weakening your organization's security.

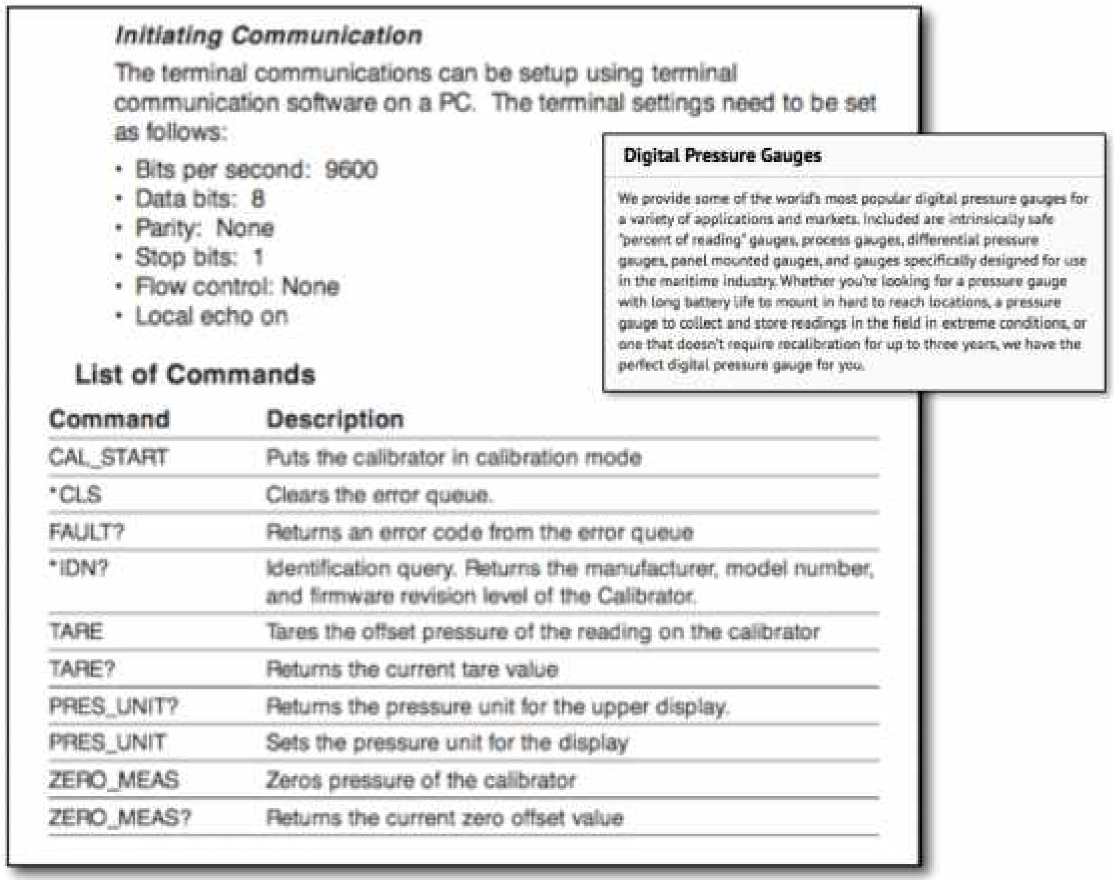
Analysis presented will discuss the real risk associated with different types of instrumentation and devices, network topologies, and technologies used in smart devices and systems. Additionally, we will analyze the possible effects on safety systems and how to compensate for them and how to protect your systems.

Key words: Calibration Risks, Calibration Cybersecurity Risks, Malware Insertion

Introduction: It is common to find microprocessors in virtually everything including the instruments we are using in our facilities. The microprocessor has made significant impacts in performance and communications and might be weakening your organization's security. The simple act of sending the instrument to a third party for calibration might be compromising your facility's cybersecurity posture.

The smart instruments include a microprocessor and memory where firmware that runs code to operate the instrument resides. Many of these devices were designed and built without much concern for cybersecurity. If an instrument designed without following strict cybersecurity rules for both the firmware, memory management and communications is calibrated by connecting to a system where malware is present, then the malware could potentially migrate to the instrument. Reconnecting the instrument after calibration might introduce malware into your facility, thereby placing your entire operation at risk.

Smart Instruments: Many instruments are simple devices and lack the ability to store and pass a payload like malware. Malware, unwanted and often malicious code, will require a certain amount of memory to store itself in and then a communications method to get from the instrument into the network. Looking for potential risk can be as easy as looking at the specifications or in the manual for directions like the image below in Figure1.



Initiating Communication

The terminal communications can be setup using terminal communication software on a PC. The terminal settings need to be set as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None
- Local echo on

Digital Pressure Gauges

We provide some of the world's most popular digital pressure gauges for a variety of applications and markets. Included are intrinsically safe "percent of reading" gauges, process gauges, differential pressure gauges, panel mounted gauges, and gauges specifically designed for use in the maritime industry. Whether you're looking for a pressure gauge with long battery life to mount in hard to reach locations, a pressure gauge to collect and store readings in the field in extreme conditions, or one that doesn't require recalibration for up to three years, we have the perfect digital pressure gauge for you.

List of Commands

Command	Description
CAL_START	Puts the calibrator in calibration mode
*CLS	Clears the error queue.
FAULT?	Returns an error code from the error queue
*IDN?	Identification query. Returns the manufacturer, model number, and firmware revision level of the Calibrator.
TARE	Tares the offset pressure of the reading on the calibrator
TARE?	Returns the current tare value
PRES_UNIT?	Returns the pressure unit for the upper display.
PRES_UNIT	Sets the pressure unit for the display
ZERO_MEAS	Zeros pressure of the calibrator
ZERO_MEAS?	Returns the current zero offset value

Figure 1

Words like digital, smart, wireless, and IoT (Internet of Things) in the description of a device, are clues that their might be a method to accidently or deliberately load a malware payload onto the instrument. If the instrument has a digital communications port or capability (wireless), it is a potential threat.

Background: To our knowledge, malware has not migrated using instruments as of the writing of this paper. However, it is entirely possible for this to occur and it requires an awareness to prevent the malware insertion from occurring.

Malware has been inserted into many facilities to date and has caused significant damage including complete loss of control. Malware easily migrates across digital connections including wired and wireless communications. It would be easy enough for a nation state or sponsored entity to create malware to take advantage of instrumentation to gain access to secure systems. Unfortunately, every threat vector must be considered in today's environment.

We already know malware can be carried in using a USB memory device. We also know from www.KrebsOnSecurity.com distributed denial of service (DDoS) attack, that the malware called "Mirai" that caused to DDoS attack resided in IoT devices like routers, IP cameras, and digital video recorders (DVRs). This type of malware scans connected devices looking for suitable devices to install itself on and spread further. This type of code typically uses a brute force username and password method to access the device.

We discovered with "Mirai" that it took advantage of devices that had weak or published user names and passwords. Most of the infected devices had no way to change the username or password built into their firmware and even if they did, most people do not change them because they are simple devices. An IP camera's username and password seems irrelevant in a world where most people do not have passwords on their cellphones. Unfortunately, this is the same problem we see in many industrial facilities. Many operation personnel and management insist that the same password and username be used for everyone, or they insist that none be used, and in many cases the user name and password is the default so that they can find it in an emergency. Unfortunately, this is exactly the weakness that Mirai utilized and it will make it easier for the next malware to take advantage of your control system.

If unwanted code known as malware finds its way into your instrumentation, some malware types can cause harm by itself like erasing the boot sector on a hard disk drive, but malware commonly communicates with a command and control (CIC) server somewhere in the world plugged into the Internet. The command and control server may just collect intelligence or it might facilitate the insertion of a larger payload (more powerful malware) or allow for an attacker to take remote control. The Ukraine power grid attack was a remote-control man-in-the-middle attack which removed control and visualization from operators followed by destroying the disk drives afterwards. The Saudi Aramco attack called Shamoon (or Disttrack), uploaded files from 35,000 computers before erasing the files and then destroying the disk drives. Both attacks had devastating results. And if you are assuming instrumentation isn't a target because of it small processor and memory foot print, the US Government Aurora Generator Test which destroyed a power generator in 2007, was only 21 lines of code.

Best Practices: Protecting your systems is one more ongoing engineering project. It requires common sense and good procedures designed to prevent the insertion. We will not stop using the microprocessor based devices, so we need to get smarter about how we use them and protect them.

Practical steps include identifying what instruments you have onsite and which ones are digital followed by which ones are calibrated externally. We might need to define the calibration instruments we use in calibration too, especially if they are sent out or connected externally to calibrate or update.

Once each instrument is identified and classified, the threat from each could be assessed also. An instrument inside of a critical process that is carefully isolated and sent out for calibration, should warrant further investigation.

Investigation should include understanding the vendor’s methods for insuring the smart instrument is secure and will remain secure. This should include verifying methods used during design and programming and any third-party certification granted. If the instrument or calibration tool is updated through a website, then what effort has the vendor made to insure the website and update does not become corrupted.

The IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities should be followed for the design of the embedded electronic devices that are utilized in critical infrastructure. If you consider your process critical, even if the government does not, then you might want to consider using devices that meet this criterion also.

Likewise, the ISA100 Wireless Compliant registration is a very good list of vendor products that are taking wireless communications seriously.

Unfortunately, none of these guarantee that your instruments and connected systems are safe from malware. Good practice would dictate we use caution in addition to using instruments from trusted and verified sources. Caution should include verifying the testing facility and the procedures used both internally and externally.

Conclusion: Awareness of cybersecurity is growing. As more and more vendors bring products out that have better security, we will not be able to relax our own security efforts because the threat will also evolve. Thinking logically about devices, especially devices that have a communications port other than a 4-20ma or 0-10v signal, will need to be treated as potentially a threat.

A practical reality is that a sophisticated instrument with massive memory and computing power that doesn’t connect to a communication network is not really a risk the systems. But a simple instrument with a microprocessor connected to the system might bring the entire process down.