

Attachment GPR-02

Cyber-Informed Engineering (CIE) Analysis Guidance

This guidance document is intended to assist recipients and engineers with developing a Cyber-Informed Engineering (CIE) analysis. A CIE analysis is required only when committed to by recipients in their letter of interest (LOI), and therefore a requirement of the funding agreement. However, DEQ encourages all communities and consultants to consider completing a CIE analysis.

This guidance does not represent a comprehensive cybersecurity standard, nor does it replace professional engineering judgment, legal advice, or specialized cybersecurity expertise. Recipients are encouraged to engage qualified professionals such as licensed engineers with cybersecurity experience or firms specializing in CIE, operational technology (OT) cybersecurity, or industrial control system (ICS) security to prepare, review, or supplement a CIE analysis.

These CIE analyses may be exempt from disclosure from a public records request as critical infrastructure in accordance with Idaho Code § 74-105(4)(b). DEQ does not evaluate or certify the technical adequacy, engineering validity, cybersecurity effectiveness, operational feasibility of any proposed controls, strategies, legal conclusions or recommendations in a CIE analysis.

A CIE analysis can be part of either a planning grant or a SRF construction project. Recipients are encouraged to begin developing this analysis early in the planning and design phase of the project. Additional information about DEQ's SRF program is found in the [Grants and Loans Program Customer Handbook](#). To satisfy DEQ's funding requirements, follow the steps below to develop a CIE analysis:

Step 1 – Identify and list systems and equipment from the selected project that will be at risk of cyberattack:

- What systems and equipment are potentially accessible to cyberattacks (i.e., is there an electronic interface that communicates information in and out)? **Figure 1** shows this relationship between information technology, operational technology, and industrial control systems.
- What is the critical function of the systems and equipment in scope?
- Which systems and equipment provide controlling actions that execute the critical function?
- What IT security is in place on the system or equipment? For example, multifactor authentication or password protocols. See AWWA's "[Getting Started Guide](#)" and "[Assessment Tool](#)."

Step 2 – Assume the security controls for the system and equipment listed in Step 1 are breached and the automation systems become unreliable or unavailable. Describe the resulting impacts. The most common individual [equipment](#) and [systems](#) are provided in the [CIE Examples](#) section below. Key considerations include, but are not limited to, the following:

- What is the worst thing that can happen, and could it be catastrophic?

- How would the operators respond to a cyberattack?
- If a system sustains a cyberattack, how long can that system and equipment be down or unreliable?
- Where could adversary manipulation of data lead to operational or safety impacts?

Step 3 – Discuss and develop CIE control recommendations that would limit or eliminate the potential impacts from cyberattack identified in Step 2. Key considerations include, but are not limited to, the following:

- How can the system or equipment be run without automation while balancing operational flexibility?
- What engineered controls would reduce or eliminate the potential impacts from cyberattack?
- Could the equipment be isolated from any network communications and remain operational?
- How will monitoring be used to validate data in the process?
- Are there features in the system or equipment that are not absolutely necessary and can be replaced with simpler systems or equipment?

Step 4 – Submit CIE analysis to DEQ for review and approval:

- Planning Grants—Incorporate the CIE analysis as a standalone chapter or section of the final planning document and submit to DEQ.
- SRF Construction Loans—Incorporate the CIE analysis into the project preliminary engineering report (PER), plans and specifications, then submit to DEQ.

Cybersecurity IT, OT & ICS

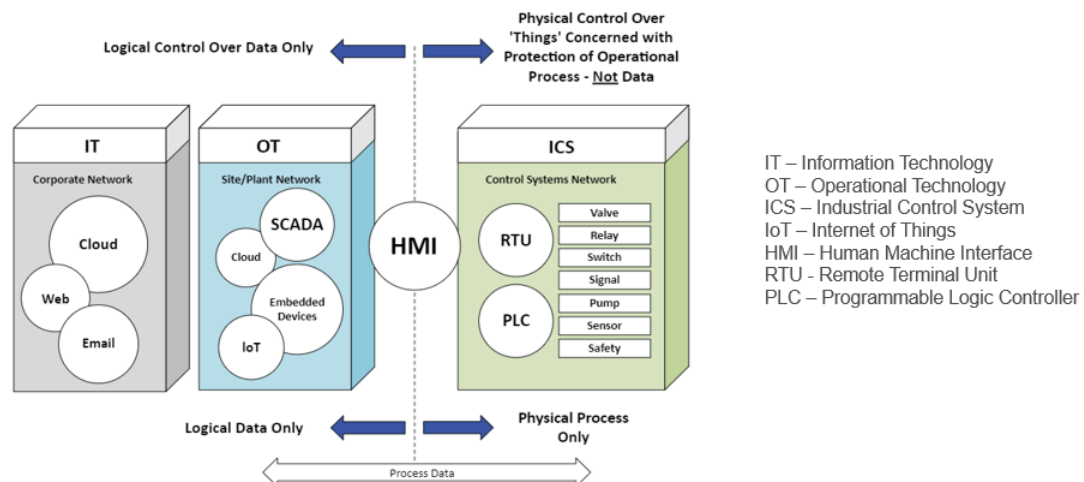


Figure 1. Cybersecurity controls for IT, OT, and ICS.

CIE Examples

Locating your system and equipment for a CIE analysis: The most common equipment and systems are provided in this section. Click on the individual equipment and systems to review common considerations of a CIE analysis and how it may apply to your project. If you do not see your project equipment or systems listed, contact DEQ's Grants and Loans Bureau to assist you with developing the content.

General Systems:

- [Chemical Feed](#)
- [Package System](#)
- [Pump Station](#)
- [Sedimentation](#)

Drinking Water Systems:

- [Filters](#)
- [Pressure Reducing Station](#)
- [Water Storage Reservoir](#)

Wastewater Systems:

- [Aeration Systems](#)
- [Digester](#)
- [Headworks](#)

Equipment:

- [Blower](#)
- [Boiler](#)
- [Chemical Pump](#)
- [Chemical Tank](#)
- [Compressor](#)
- [Float Switch](#)
- [Flow Meter](#)
- [Level Sensor](#)
- [Mixer](#)
- [Oxygen Sensor](#)
- [Pressure Sensor](#)
- [Pressure Switch](#)
- [Pump](#)
- [Storage Tank](#)
- [Valve](#)
- [Variable Frequency Drive](#)
- [Vibration Sensor](#)

Additional Resources and Training

CIE Resources

- **CIE Strategy** - [https://www.energy.gov/sites/default/files/2022-06/FINAL DOE National CIE Strategy - June 2022 0.pdf](https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022%200.pdf)
- CIE Implementation Guide - <https://www.osti.gov/biblio/1995796>
- CIE Water Booster Pump Station Case Study:
 - **Workbook:** <https://www.osti.gov/biblio/2371031>
 - **Slides:** <https://www.osti.gov/biblio/2447693>
- **AWWA Book** - "[Resilience Through Cyber-Informed Engineering: An Engineering and Operations Approach to Cybersecurity](#)"
- **AWWA Guidance** - "[Cybersecurity Risk Management Getting Started Guide](#)"
- **AWWA "Cybersecurity & Guidance Assessment Tool"**

CIE Training

- CIE Quarterly Webinar: What is Cyber-Informed Engineering – June 27, 2024
<https://www.youtube.com/watch?v=P4dpA7-vjig>
- Idaho Department of Environmental Quality Dec 2024 Webinar - [IDEQ CIE webinar recording](#)
- Idaho National Laboratory (INL) Jan 2025 Webinar [INL CIE for the Water Sector webinar](#)

Systems

General Systems

Chemical Feed

Typical Equipment

Chemical systems can include a [chemical tank](#), [chemical pump](#), and [flow meter](#). Navigate to the [Equipment](#) section to view additional equipment that could be in the chemical system.

Potential Impacts

- The chemicals could be manipulated to overdose or underdose the chemical via the chemical pump or the chemical tank. Manipulating the chemical dosage could create a health hazard if there is too much or too little chemical fed. The chemical feed from the tank could be manipulated to dose the entire tank volume in a short period of time.
- The flow meter signal could be manipulated to show low or high flow, altering the dosing pace.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a separate flow sensor that reports the flow in the system, independent of the primary flow meter.
- Send alarm data only to the Supervisory Control and Data Acquisition (SCADA) system, and wire start/stop signals directly to the pump controller. Alarms should have on-site visual or audible annunciation.
- Install a day tank. See [Chemical Tank](#) equipment.
- Use an isolated chemical sensor to determine if there is too little or too much chemical sensed in the system. Alarms should have on-site visual or audible annunciation. Send the alarm signals only to SCADA.
- Interlock the chemical feed pump to a pump run signal, which only allows the chemical feed pump to operate when the pump is running. This signal should be hardwired from the pump controller to the chemical feed pump.
- Send an alarm if the chemical pump is running and the pump is off. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Package System

Typical Equipment

Package systems can include a variety of equipment. This section provides a generic description and guidance. Navigate to the [Equipment](#) section to view equipment that could be part of the package system.

Potential Impacts

- The vendor could “require” remote access to the equipment for updates and troubleshooting, which exposes the equipment to external manipulation.
- The vendor may access multiple systems from the same computer, exposing the computer to viruses and providing an avenue of attack.
- Equipment in the package system could have been compromised before installation at the site.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Limit vendor access to the system controlling the programmable logic controller (PLC) .
- Have update files loaded on site, at the PLC.
- If remote access has to occur, set a specific time frame where remote access is granted.
- Have a recovery plan in case the controlling PLC is compromised.
- Have the vendor provide a CIE analysis on the equipment in their package system and provide appropriate controls to protect against a cyberattack.

[Back to CIE Examples](#)

Pump Station

Typical Equipment

Pump stations can include [pumps](#), [variable frequency drives](#), [chemical tank](#), [chemical pump](#), [level sensor](#), [pressure sensor](#), and [flow meter](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the pump station.

Potential Impacts

- The pump operation could be attacked to stop the pump from running, starting, and stopping rapidly; controlling variable frequency drive (VFD) speed; and manipulating the flow meter value. Starting and stopping the pump rapidly could generate water hammer at the pump. If there are multiple pumps, starting all the pumps together could create cavitation in the pump/pipes resulting in catastrophic failure.
- The chemicals could also be manipulated to overdose or underdose the chemical via the chemical pump or the chemical tank. Manipulating the chemical dosage may create a health hazard if there is too much or too little chemical fed.
- The level sensor signal could be manipulated to show low or high level, altering the system operation.
- The pressure sensor signal could be manipulated to show low or high pressure, altering the system pressure or rapid cycling of the controlled equipment.
- The flow meter signal could be manipulated to show low or high flow, altering the system pressure or chemical dosing required.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a time delay relay to protect the pump from starting and stopping too quickly. Alarm data is sent only to SCADA, which is wired directly to the pump controller. Alarms should have on-site visual or audible annunciation.
- Interlock the run commands from redundant pumps to prevent all of them from starting at the same time. The interlock run commands should be hardwired using control relays and the VFD input and output terminals. Install manual lead lag switches and manually rotate pumps on a regular schedule.
- Protect the chemical system so the correct dosing is applied. See [Chemical Feed](#) systems.
- Protect the flow meter signal from over or under reporting the flow. See [flow meter](#) device below.
- The VFDs could be manipulated. See [variable frequency drives](#) for more information.

[Back to CIE Examples](#)

Sedimentation

Placeholder, not sure what critical equipment should be listed and would this system be considered critical

[Back to CIE Examples](#)

Drinking Water Systems

Filters

Typical Equipment

Filter systems can include [flow meters](#), [pumps](#), [storage tanks](#), [pressure sensors](#), [chemical tank](#), [chemical pump](#), and [valves](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the filters.

Potential Impacts

- The filter system operation could be attacked by manipulating the flow meter value, valve operation, or reported storage tank level.
- The flow meter value could report high or low, altering the effectiveness of the system.
- The filter system pumps could be turned off or all started together.
- The valves could be opened or closed, causing negative effects on the system.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a separate flow sensor that reports the flow in the system, independent of the flow meter. Additionally, a flow switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA; wire start/stop signals directly to the controller. Alarms should have on-site visual or audible annunciation.
- Install a separate pressure sensor that reports the pressure in the system, independent of the pressure meter. Additionally, a pressure switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA; wire start/stop signals directly to the controller. Alarms should have on-site visual or audible annunciation.
- Interlock the run commands from redundant filter pumps systems and backwash systems to prevent all of them from starting at the same time. The interlock run commands should be hardwired using control relays and the pump motor input and output terminals. Install manual lead lag switches and manually rotate pumps on a regular schedule.

- Provide valves with the ability to be manually operated, without any PLC control.

[Back to CIE Examples](#)

Pressure Reducing Station

Typical Equipment

Pressure-reducing stations can include [pressure sensors](#) and [valves](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the pressure reduction station.

Potential Impacts

- The system operation could be attacked by manipulating the pressure sensor value or the valve operation. The pressure sensor value could report high or low, altering the effectiveness of the system.
- The valves could be opened or closed, causing negative effects on the system.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a separate pressure sensor that reports the pressure in the system, independent of the controlling sensor. Additionally, a pressure switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Water Storage Reservoir

Typical Equipment

Water storage reservoirs can include [level sensors](#), [pumps](#), [variable frequency drives](#), and [valves](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the pump station.

Potential Impacts

- The system operation could be attacked by manipulating the level sensor value.
- The level sensor value could report high or low, altering the effectiveness of the system.
- Manipulation could also lead to the reservoir overfilling and cause a catastrophic failure.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a separate level sensor that reports the level in the system, independent of the controlling sensor. Additionally, a level switch, hardwired directly to the controlling equipment, could provide high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA. Alarms should have on-site visual or audible annunciation.
- Interlock the run commands from redundant pumps to prevent all of them from starting at the same time. The interlock run commands should be hardwired using control relays and the pump motor input and output terminals. Install manual lead lag switches and manually rotate pumps on a regular schedule.

[Back to CIE Examples](#)

Wastewater Systems

Aeration Systems

Typical Equipment

Aeration systems can include [compressors](#) and [oxygen sensors](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the aeration system.

Potential Impacts

- The aeration operation could be attacked by stopping the compressors, stopping the compressors from starting, or manipulating the oxygen level sensor value.
- The oxygen level sensor signal could be manipulated to show high or low oxygen levels, affecting the aeration operation.
- If the compressors are stopped, it would alter the coarse bubbler diffuser operation.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a mechanical or separate oxygen sensor that sends alarms to SCADA, indicating a high or low level state. Alarm data is sent only to SCADA, wired directly to the compressor's controller. Alarms should have on-site visual or audible annunciation.
- Use a handheld meter to measure dissolved oxygen and compare it to the sensor readings. Add the measurement step to a weekly testing procedure.
- Provide oxygen sensors downstream to check the process and provide additional monitoring. Alarm and status signals are sent only to SCADA.

[Back to CIE Examples](#)

Digester

Typical Equipment

Digesters can include [blowers](#), [variable frequency drives](#), [mixers](#), [boilers](#), and [flow meters](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the digester.

Potential Impacts

- The digester operation could be attacked by altering the heat parameters, stopping the mixer, controlling VFD speed, and manipulating the gas flow meter value.
- The flow meter signal could be manipulated to show low or high gas flow, affecting the boiler operation.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a secondary temperature sensor that sends alarms to SCADA if the temperature varies from the controlling temperature sensor. Additionally, a temperature switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA, wired directly to the pump controller. Alarms should have on-site visual or audible annunciation.
- Protect the VFDs from manipulation. See [variable frequency drives](#) for more information.

[Back to CIE Examples](#)

Headworks

Typical Equipment

Headworks can include Influent [pumps](#), [variable frequency drives](#), and [level sensors](#). Navigate to the [Equipment](#) section to view additional equipment that could be located at the headworks.

Potential Impacts

- The headworks operation could be attacked by stopping the screens, stopping the backwash pumps, and manipulating the influent level or flow sensor value.
- The influent level sensor meter signal could be manipulated to show high or low influent levels, affecting the headworks operation.

Example CIE Controls

Click the typical equipment links above for specific protection examples.

- Install a mechanical level sensor (i.e., float switch) that sends alarms to SCADA on a high level state. Alarm data is sent only to SCADA, wired directly to the pump controller or screens. Alarms should have on-site visual or audible annunciation.

- Install air quality monitoring to check for gas accumulation in the headworks. Alarm data is sent only to SCADA. Alarms should have on-site visual or audible annunciation.
- Protect the VFDs from manipulation. See [variable frequency drives](#) for more information.

[Back to CIE Examples](#)

Equipment

Blower

Potential Impacts

- Manipulating the blower operation, start and stop.

Example CIE Controls

- Install a sensor that detects the blower air flow. Alarm data is sent only to SCADA, wired directly to the blower controller to maintain optimal operation. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Boiler

Potential Impacts

- Manipulating the boiler operation could result in temperature operation outside of the specified design parameters and could also start back-up boilers when not called to run.

Example CIE Controls

- Install an additional temperature sensor that compares its reading to the SCADA temperature sensor. Additionally, a temperature switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA, wired directly to the pump controller. Alarms should have on-site visual or audible annunciation.
- Interlock the run commands from redundant pumps to prevent all of them from starting at the same time. The interlock run commands should be hardwired using control relays and the pump motor input and output terminals.

[Back to CIE Examples](#)

Chemical Pump

Potential Impacts

- Controlled by an analog signal and needs protection from manipulation and overdosing or underdosing.

Example CIE Controls

- Inline monitoring of chemical level downstream of the chemical pump and alarm if levels are out of range. Do not allow control through SCADA; use monitoring and alarming only. Alarms should have on-site visual or audible annunciation.
- Right-size chemical feed pump to limit the range of operation.

[Back to CIE Examples](#)

Chemical Tank

Potential Impacts

- Manipulating the chemical release could release the entire tank of chemicals.

Example CIE Controls

Install a day tank that is manually filled, or autofill with an interlocked time delay, from the chemical tank. Limit the amount of chemical released. Use redundant tanks and back-up starts if no chemical is detected, which protects the chemical from being turned off. Alarm is sent to SCADA and should have on-site visual or audible annunciation. Install an interlocked time delay relay to prevent the day tank valve from operating too often. Isolate the time delay relay from SCADA control and only report status or alarms to SCADA.

[Back to CIE Examples](#)

Compressor

Potential Impacts

- Manipulating the compressor gas release rate.

Example CIE Controls

Install a back-up compressor; back-up starts if no gas is detected, protecting the gas from being turned off. Alarm is sent to SCADA and should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Float Switch

Potential Impacts

- The status signal is only run through the PLC for equipment control.

Example CIE Controls

- Install a mechanical relay and route one status signal to the PLC and the other status signal is routed directly to the equipment controller. The switch can operate the equipment, independently of the PLC. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Flow Meter

Potential Impacts

- Manipulating the sensor data or turning the sensor off.

Example CIE Controls

- Install a flow-sensing device, not controlled by SCADA, that sends flow status and alarm data only to SCADA. Alarms should have on-site visual or audible annunciation. Additionally, a flow switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal.

[Back to CIE Examples](#)

Level Sensor

Potential Impacts

- Manipulating the sensor data or turning the sensor off.

Example CIE Controls

- Install mechanical switches (i.e., float switches) to indicate a high, high-high, low, or low-low states. Install a mechanical relay and route one status signal to the PLC and the other status signal is routed directly to the equipment controller. The switch can operate the equipment, independently of the PLC. Alarm is sent to SCADA and should have on-site visual or audible annunciation.
- Install a separate level-sensing device, not controlled by SCADA, that sends flow status and alarm data only to SCADA. Alarms should have on-site visual or audible annunciation.
- .

[Back to CIE Examples](#)

Mixer

Potential Impacts

- Manipulating the mixer operation, start and stop.

Example CIE Controls

- Monitor if the mixer fails to start or fails to stop with mechanical relays. Alarm data is sent only to SCADA, wired directly to the mixer controller to maintain desired operation. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Oxygen Sensor

Potential Impacts

- Manipulating the sensor data or turning the sensor off.

Example CIE Controls

- Install an isolated oxygen sensor that senses an over or under oxygen event. Alarm data is sent only to SCADA, wired directly to the motor controller. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Pressure Sensor

Potential Impacts

- Manipulating the sensor data or turning the sensor off.

Example CIE Controls

- Install a pressure switch to mitigate an over or under pressure event. Install a mechanical relay and route one status signal to the PLC and the other status signal is routed directly to the equipment controller. The switch can operate the equipment, independently of the PLC.
- Alarm data is sent only to SCADA, wired directly to the motor controller. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Pressure Switch

Potential Impacts

- The status signal is only run through the PLC for equipment control.

Example CIE Controls

- Install a mechanical relay and route one status signal to the PLC and the other status signal is routed directly to the equipment controller. The switch can operate the equipment, independently of the PLC. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Pump

Potential Impacts

- Manipulating the pump operation could result in water hammer if restarted too quickly and could also start back-up pumps when not called to run.

Example CIE Controls

- Install a time delay relay to protect the pump from starting and stopping too quickly. Alarm data is sent only to SCADA, wired directly to the pump controller. Alarms should have on-site visual or audible annunciation.
- Interlock the run commands from redundant pumps to prevent all of them from starting at the same time. The interlock run commands should be hardwired using control relays and the pump motor input and output terminals.

[Back to CIE Examples](#)

Storage Tank

Potential Impacts

- Manipulating the level sensor to show the incorrect volume of liquid in the tank.

Example CIE Controls

- Install mechanical switches (i.e., float switches) to act as a high, high-high, low, or low-low levels in the tank.
- Alarm data is sent only to SCADA, wired directly to the valve or pump controller. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Valve

Potential Impacts

- Manipulating the valve position or operation could result in pipe cavitation.

Example CIE Controls

- Install a time delay relay to protect the valve from operating too often. Alarm data is sent only to SCADA, wired directly to the valve controller. Alarms should have on-site visual or audible annunciation.
- Install a limit switch to limit valve operation range. Alarm data is sent only to SCADA, wired directly to the valve controller. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)

Variable Frequency Drive

Potential Impacts.

- Manipulating the VFD speed or operation could result in over or under operation of the associated equipment.

Example CIE Controls

- Install a time delay relay to protect equipment from operating too often. Alarm data is sent only to SCADA, wired directly to the valve controller. Alarms should have on-site visual or audible annunciation.
- Have VFD critical data signals hardwired to SCADA for reporting. Limit or eliminate direct VFD control via the internet.
- Program the VFD for a soft stop operation and ramp down the VFD when called to stop.
- Install a speed limit switch to limit VFD operation range. Alarm data is sent only to SCADA, wired directly to the VFD or equipment controlled. Alarms should have on-site visual or audible annunciation.
- If the VFD is not using an analog signal for VFD speed, the VFD could be operated as a soft start motor starter, ramping up the motor to reduce the starting current.
- Do not allow reprogramming of the VFD via SCADA. VFD programming is only performed at the physical location.

[Back to CIE Examples](#)

Vibration Sensor

Vulnerability

- Manipulating the sensor data or turning the sensor off.

Example CIE Controls

- Install a vibration switch to mitigate an over or under vibration event. Additionally, a vibration switch, hardwired directly to the controlling equipment, could indicate high or low conditions and generate an alarm signal. Alarm data is sent only to SCADA, wired directly to the motor controller. Alarms should have on-site visual or audible annunciation.

[Back to CIE Examples](#)