PreventOTPhysDamage: Anticipating and Preventing Catastrophic OT Physical Damage Through System Thinking Analysis

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Matt Angle <mangle@mit.edu>, Stuart Madnick <smadnick@mit.edu>, James L. Kirtley <kirtley@mit.edu>, Nabil Sayfayn <sayfayn@hotmail.com>

Massachusetts Institute of Technology — MIT MANAGEMENT SLOAN SCHOOL

Cybersafety Analysis of Energy Systems

INTRODUCTION

To date, most attacks on Energy Systems have either targeted the IT infrastructure (e.g., the Aramco Shamoo attack) or circuit breakers of the Operational Technology (e.g., the Ukraine attack.) In such cases, recover is usually quite fast – either by rebooting the IT computers or resetting the breakers.

But, if the Operation Technology equipment, especially the important, large, customized equipment, is physically damaged, recovery can take weeks or even months.

Aurora was a **2007 Department of Homeland Security** investigation in to the **vulnerability of the US power grid** to cyber attacks. The program culminated in a demonstration of the destruction of a diesel generator (shown below) by changing the code associated with the synchronization of the generator to the grid. By causing switches which connect the generator to the grid to close at the wrong time, mechanical shocks destroyed the generator.

In 2008, a malicious group was able to penetrate the network at a pumping station on **a pipeline in Turkey**. By changing control settings, they were able to blind the monitoring systems and cause a situation which overpressurized the lines, resulting in an explosion and fire, shown in the picture below on the left.

STUXNET is a worm that was created presumably to disrupt **Iranian enrichment** of Uranium. The worm traveled through Windows computers looking for the Siemens STEP7 control software. It would then migrate to an associated programmable logic controller (PLC), where it would look for a certain make and model of variable frequency drive (VFD). In this way, precisely attacked its intended target. If this drive was programmed to operate in a specific frequency range, Stuxnet would command it to raise and lower the frequency, driving centrifuges to failure (see picture above right.)

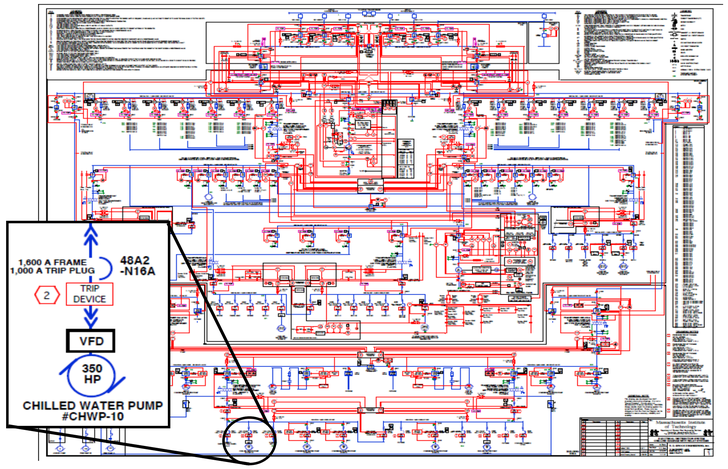
In December 2015, the **Ukranian power grid** was the victim of a cyber attack that managed to penetrate the network controlling the physical hardware in the grid, opening switches at substations while overwriting firmware in devices used to control the hardware and wiping the drives of computers used to control the system.

The MIT Central Utilities Plant

The MIT Central Utilities plant contains a 21 MW gas turbine generator used to provide electricity for the MIT campus. Waste heat is used to fire boilers that produce steam for campus heating and to drive chillers which provide chilled water and air conditioning. The plant is connected to the power grid in Cambridge, and the plant's generation capability is throttled to most economically supply power based on fluctuating electricity and natural gas prices.

Recently, a water/fuel injection nozzle was clogged as a result of a contaminated filter (not caused by cyber). As a result, the turbine was down for 3 months while replacement parts were sourced from the manufacturer in Germany. The point is: **repairs can take a long time**.

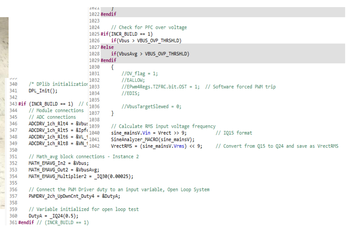
Below is a wiring diagram of the MIT campus, showing pumps that keep chilled and hot water flowing on campus, switches that distribute electricity to campus, and all of the major electrical loads on campus. Many of these components use **Variable Frequency Drives (VFDs),** as highlighted in the diagram, and are automated and controlled remotely from a control room at the Central Utilities plant. This facility makes for an excellent study of vulnerabilities in the US power grid at large.



Many ways to access the controls of the various systems exist. Each of the control units on the more modern pieces of hardware (chillers, turbines) has a remote monitoring system installed by the manufacturer with a communication line out. Some versions of these systems have only remote monitoring capability, while others have remote control authority. Various strategies exist for isolating them from remote commands, but at the expense of the inability to use common two-way communication protocols, such as TCP/IP. Outside contractors are used to maintain various systems, including the VFDs that drive all of the larger pumps in the system.

A Small-scale Demonstration

To demonstrate vulnerability of energy storage elements to software control, a small-scale test on a **variable frequency drive (VFD)** was performed. A VFD often used in lab to create custom motor drives for research purposes was selected, as the source code for the firmware is provided.



This particular VFD features a power factor correction stage, a functionality required by more and more government regulations. This topology is also known as a boost converter. Software controls are used to control this device to regulate voltage on the DC bus.

With a few simple code changes, the protections built in to software are disabled. The voltage on the DC bus rises to the point where it damages the electrolytic capacitors on the bus, causing dielectric breakdown and an arc that burns until it destroys the structure of the capacitor, often with dramatic results. After the capacitors burn, the voltage on the bus continues to climb until it destroys the switches that drive the output of the VFD. The results of this small test are shown in the picture below left.

VFDs are increasingly connected to the internet for remote commissioning and even for remote firmware updates. The mechanical devices controlled by the VFDs may also be attacked by changing configuration settings. This attack is easily scaled to larger VFD-controlled devices, such as the ones in the photo above right.

RESEARCH GOALS

- **Our analysis and mitigation approach uses a top-down system-theoretic analysis which focuses on what mishap(s) you are trying to prevent.**
- **The overall system is viewed as a hierarchy of control loop structures where constraints at a higher level control behavior at lower levels.**
- **We identify hazards, not yet been exploited, such as the VFDs, and determine hierarchy of controls to mitigate.**
- **We are applying this method for forward-looking hazard prevention, initially with the MIT Central Utilities Plant.**
- **We seek other energy organizations to demonstrate and validate its effectiveness => Please contact us.**