MIT MANAGEMENT SLOAN SCHOOL

INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY $(IC)^3$

Identifying and Mitigating Cyber Attacks that could cause Physical Damage to Industrial Control Systems

Matthew G. Angle
Stuart Madnick
James L. Kirtley, Jr.

Working Paper CISL# 2017-14

August 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Identifying and Mitigating Cyber Attacks that could cause Physical Damage to Industrial Control Systems

Matthew G. Angle, Member, IEEE, Stuart Madnick, Member, IEEE, James L. Kirtley, Jr., Fellow, IEEE

***Abstract*-- Physical industrial control systems are increasingly controlled by reconfigurable, network-enabled devices to increase flexibility and ease commissioning and maintenance. Such capability creates vulnerabilities. Devices may be remotely reprogrammed by a malicious actor to act in unintended ways, causing damage to mechanical equipment, infrastructure, and life and limb. In this paper, a few examples of actual damage to cyber-physical systems are shown and a small scale version of an attack on ubiquitous equipment is demonstrated.**

***Index Terms*--The author shall provide up to 10 keywords (in alphabetical order) to help identify the major topics of the paper. The thesaurus of IEEE indexing keywords should be referenced prior to selecting the keywords to ensure that the words selected are acceptable. The thesaurus is posted at http://www.ieee.org/organizations/pubs/ani_prod/keywrd98.txt.**

I. Nomenclature

A nomenclature list, if needed, should precede the Introduction.

II. Introduction

PHYSICAL control systems are increasingly tied to the internet to enable remote monitoring and control, creating new vulnerabilities. Intended to allow simplification of product lines and ease of installation and commissioning, product flexibility introduces the potential for misuse. No longer limited to stealing credit cards, data, or other personal information, hackers or other malicious actors may now remotely access hardware, change settings, or reprogram devices to cause real physical damage on an unlimited scale.

III. Background

A few selected examples show the breadth of the problem's motivations, methods, and potential impacts. The Aurora Vulnerability, a United States Department of Homeland Security program established a potential vulnerability. In other examples, the power grid in the Ukraine was brought down for a short time, a pipeline in Turkey was blown up, and malicious computer worm halted the Iranian nuclear fuel enrichment program.

A. Aurora Vulnerability

The so-called "Aurora Vulnerability" was demonstrated at Idaho National Labs as part of a 2007 Department of Homeland Security investigation of vulnerabilities in the United States power grid. In the test, researchers used remotely-controllable relays to connect and disconnect a diesel backup generator to the grid. The test resulted in the complete destruction of the generator unit [1].

To understand the mechanism of attack requires an understanding of generator synchronization. Generator synchronization is required to connect a generator to the grid. The states of the grid and generator are determined by two parameters: voltage and phase. Rotating electric machinery produces an alternating current waveform of the form V sin(ωt), Where V is the amplitude of the voltage, and ω is the frequency at which it oscillates. In the United States, this frequency is 60 Hz, or approximately 377 radians per second. The three phases are separated by 120°, forming a balanced set whose sum is zero.

If the voltage and phase of the generator do not match those of the grid when the two are connected, current will flow into the generator and produce torque sufficient to pull the generator into correct phase alignment. Generator voltage will determine whether power flows into or out of the generator. The mechanisms of these actions vary with the type of generator, but they all result in torque applied to the generator to drag it into matching phase.

To accomplish this task, an instrument called a synchroscope, shown in Fig. 2, is normally used. It shows the relative phases of the machine and grid. The operator will adjust the speed of the generator to allow the phases of the generator to align with that of the grid, at which point a switch is used to connect the two [2].

This material is based, in part, upon research supported by the Department of Energy under Award Number DE-OE0000780 and a seed grant from the MIT Energy Initiative (MITei).

Matthew G. Angle is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: mangle@mit.edu).

Stuart Madnick is with the Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: smadnick@mit.edu).

James L. Kirtley, Jr. is with the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: kirtley@mit.edu).

Fig. 1: Screen capture showing Generator used in the Aurora test.

During the Aurora test, electronic switches were used to open and close the connection of the generator to the grid. When disconnected, the generator would become unloaded, and would speed up slightly, pulling it out of phase with the grid. At this point, the switch would be reconnected, whereby power would flow into the generator, operating it as a motor to realign itself with the grid phase. The massive amount of torque stressed mechanical components in the generator. By repeatedly connecting and disconnecting the generator, mechanical components were driven to failure.

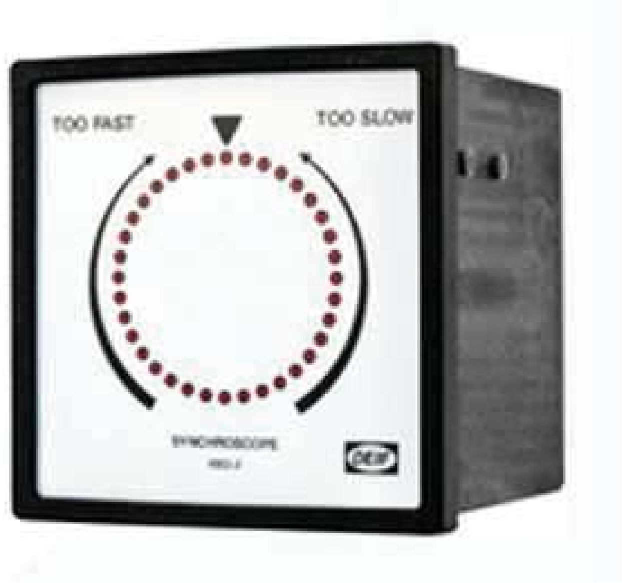


Fig. 2: Typical Synchroscope used for synchronization of electric machinery to grid

This test took advantage of a well-known and understood problem faced by industry. One example occurred at the Clinton Power Station Nuclear Plant in Clinton, IL. During a backup generator test, an out-of-phase synchronization occurred, damaging the stator windings of the generator and causing an overvoltage event on the power bus. The cause of the incident was not immediately known [3]. Other problems include breakers that close slowly, allowing the generator to move out of phase between the time that the command to close is given and the time electrical contact is made [4].

Such vulnerability is not confined to diesel backup generators. Any electrical generator that is connected to the grid will be faced with this problem, including those in wind turbines, water turbines, fossil-fuel-driven power plants, and nuclear plants.

While this event was not an attack, it demonstrated a vulnerability that could be exploited to take a power system out of commission reliably and suddenly in a manner that may not initially be recognized as an attack.

B. Ukrainian Power Grid Attack

On December 23, 2015, the lights went off in the Ivano-Frankivsk region of the Ukraine. Months before, a phishing email had been sent to workers at substations, prompting them to enable macros in an attached Word document. BlackEnergy3, a malware program, would then be installed, giving hackers a back door into the systems in the substation. From here, the attackers performed surveillance on the network, eventually obtaining login credentials for remote access to the SCADA (Supervisory Control and Data Acquisition) systems [5].

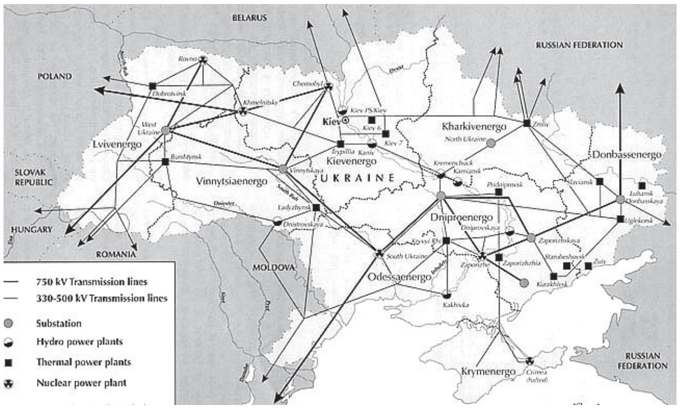


Fig. 3: Diagram of Electrical Grid in the Ukraine [6]

The attack had several different prongs. The UPS (Uninterruptible Power Supplies) that provided backup power for the control systems were disabled. Then the hackers used access to the SCADA systems to open switches which distributed power to the grid. Firmware controlling serial-to-ethernet controllers was overwritten, preventing further control of the switches. A telephone Denial-of-Service was mounted against the power utility call centers, enraging the public. Finally, a program called KillDisk was used to overwrite the computers in control centers, preventing any further action on the part of operators. While power was out for only one to six hours, seven 110 kV and twenty three 35 kV substations hit by the attack, resulting in outages to 225,000 customers, a clear message was sent [5] [7].

Months after the attack, substations were still being operated manually. While the attack merely disrupted power distribution, the potential for physical damage was there. The attackers chose only to send a message, rather than damage equipment. Russia has widely been blamed for the attack, but no one has stepped forward to claim responsibility.

C. Turkish Pipeline

Fig. 4: Explosion of oil pipeline

On August 5, 2008, an oil pipeline near Refahiye, Turkey exploded. The Turkish government initially blamed the explosion on a mechanical failure. Later, the Kurdistan Workers' Party (PKK) claimed responsibility, though it is suspected that Russia is behind the attack. The attack caused a spill of 30,000 barrels of oil and shut down the pipeline for three weeks, costing British Petroleum $5 million per day in transit tariffs and the State Oil Fund of the Republic of Azerbaijan $1 billion in lost export revenue [8].

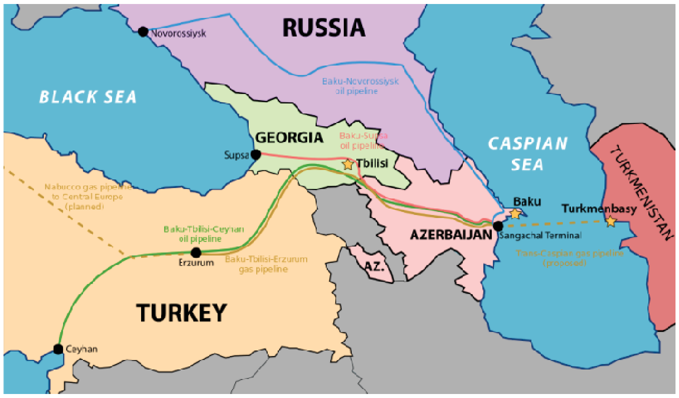

RUSSIA
Novorossiysk
Baku-Novorossiysk oil pipeline
BLACK SEA
GEORGIA
Baku-Supsa oil pipeline
Supsa
Tbilisi
CASPIAN SEA
TURKMENISTAN
Nabucco gas pipeline to Central Europe (planned)
Baku-Tbilisi-Ceyhan oil pipeline
Erzurum
Baku-Tbilisi-Erzurum gas pipeline
AZ.
Baku
Turkmenbasy
AZERBAIJAN
Sangachal Terminal
Trans-Caspian gas pipeline (proposed)
TURKEY
Ceyhan

Fig. 5: Baku–Tbilisi–Ceyhan (BTC) pipeline route

The pipeline itself was built with security in mind. Most of it is buried, and substations are surrounded with fences and barbed wire. Cameras monitor most of its length, and sophisticated alarms are present to warn of damage.

The attack was preceded by two men entering one of the substations with laptops a few days before the explosions. They were able to gain entry to the network via a vulnerability in the security cameras, from which they were able to access the computers that hosted the SCADA systems. They were able to cause the pipeline to become over pressurized, an action that may have directly led to the explosion without a secondary ignition source. The satellite communications for the alarm systems had been jammed, and the explosion was eventually reported by local residents. The security camera footage was erased, though a single thermal camera was on a different network and recorded the entry of the two men [8] [9].

This attack consisted of a deliberate act of sabotage that had measurable economic impact for multiple actors.

D. Stuxnet

Fig. 6: Iranian President Ahmadinejad during inspects centrifuges at Natanz

Stuxnet is a 500 kB worm that disrupted the Iranian Uranium enrichment centrifuges. Centrifuges are long metal cylinders that are spun at high speeds, in this case, to separate isotopes of Uranium to build nuclear weapons or to fuel power plants. These devices are run right at the mechanical limit of the cylinders, which are placed inside vacuum chambers to reduce surface drag.

Widely believed to have been developed by the United States and Israel, Stuxnet utilized four separate zero-day exploits to infiltrate SCADA systems controlling centrifuges in Iran and quietly cause failures indistinguishable from normal mechanical failures. The worm itself was only discovered long after damage had been done.

The worm worked by infecting Windows systems via the LNK vulnerability that concerned an autoplay vulnerability associated with USB sticks. It could then spread throughout a network through a vulnerability in print spoolers. From there, it would look for a copy of the Siemens Step7 software, then PLCs (programmable logic controllers) controlling certain models of VFDs (variable frequency drives) running at certain speeds corresponding to operation of centrifuges. Once the target was identified, the worm would cause the centrifuges to speed up and slow down, crossing through mechanical resonances until they failed, while simultaneously reporting normal operation back to the SCADA system. Since the Iran attacks, it has been found existing on many other systems, but with little damage to them.

Stuxnet is an attack that caused widespread damage to a system that requires only a few failures to damage the effectiveness of the whole system. Its operation was carefully tuned to produce frustrating mechanical failures that would cause delays in a large program, and it remained hidden until long after its intended damage had been done [10] [11].

E. Lessons Learned

The motivations, methods, and impacts of cyber attacks come in different flavors. The Ukranian power grid attack appears to be politically motivated and caused a relatively minor inconvenience, stopping well short of the physical damage that could have been caused with the sort of control authority obtained for the attack. The Turkish pipeline attack consisted of a much lower level of effort with real physical damage that cost many interested parties substantial amounts of money. Stuxnet was an indiscriminately-distributed piece of malware with a very specific target, designed to look like a normal mechanical failure that delayed a massive, state-sponsored research effort.

IV. Catastrophic Cyberattack to Energy Industrial Control System

Most cyber attacks to Industrial Control Systems have either targeted the IT infrastructure (e.g., the Aramco Shamoon attack) or circuit breakers of the Operational Technology (e.g., the Ukraine attack [5], [11], [13]). 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. The largest reported such attack was to the centrifuges of the Iranian uranium enrichment facility [7], [12].

To the best of our knowledge, the only demonstrated cyber attack that caused physical damage to an industrial control system was the Aurora Vulnerability, mentioned earlier. In this part of our study, we wanted to explore other vulnerabilities. We used the MIT Central Utilities Plant as a starting point for our investigation.

V. MIT Central Utilities Plant Case Study

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.

Fig. 7: Photograph of the MIT Central Utilities Plant

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 three months while replacement parts were sourced from the manufacturer in Germany. The point is that repairs can take a long time, as many components are built specifically for each installation.

Below, in Fig. 8, 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.

The plant has many points that are vulnerable to attack. The turbine itself is a large, expensive, and complicated system that may be easily damaged. It must be kept spinning while it cools to avoid damaging blades. This is accomplished by a system powered by a lead-acid battery bank. Simply disabling the charging system and monitoring alarms for this battery bank could easily cause significant damage to the turbine. Similar lead-acid battery banks exist to provide start-up power to backup generators.

The turbine is also supported by systems that regulate natural gas pressure. These are pneumatic-actuated regulators that step down pressure from a 300 PSI line pressure to a 25 PSI feed for the boilers. A loss of pneumatic pressure would, at minimum, cause a turbine shutdown. The lesson is that this complicated piece of hardware is supported by many other complicated systems, each with vulnerabilities of their own. An attack is as simple as identifying one point in one support system, and the turbine may be shut down or irreparably damaged.

Many ways to access the controls of the various systems exist. Each of the control units on the more modern pieces of hardware (chillers, turbine) 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. Industry experts that we conferred with confirmed that they do both configuration and firmware updates remotely over the internet and that the whole industry is moving that direction. 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.

The turbine, in particular, has a system installed that allows remote monitoring by the manufacturer. We were fortunate enough to talk with Siemens technicians while they were working on the turbine. They told us that there are many similar systems, and while most provide them with only remote monitoring privileges, a few allow remote engineering privileges, meaning that they can remotely control the turbine. At this time, it is unknown what is the difference between the two pieces of hardware. If this is a software configuration step, this presents a glaring vulnerability to an outsider intent on causing harm.

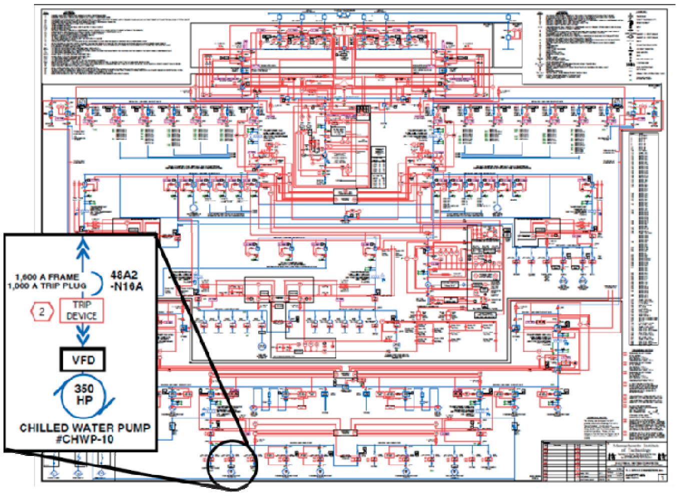


Fig. 8: Electrical layout of the MIT Central Utilities Plant

Outside contractors are used to maintain various systems, including the VFDs that drive all of the larger pumps in the system. The contractor that maintains the VFDs in the plant reports that it has never updated the firmware, but does periodically plug a laptop into the devices to monitor their operation. In some models of VFDs, a firmware update may be pushed over this same connection, and operating parameters may be changed. Either of these actions is sufficient to damage either the VFD or the load attached to it. By changing operating parameters, grossly incorrect control strategies may be imposed on physical hardware. The ability to change the firmware provides the ability to do much more or potentially non-obvious damage. In this case, infecting the computer system of the contractor may be sufficient to introduce malware into the MIT Central Utilities Plant systems.

Another outside company is used to make recommendations on turbine throttle. The plant is set up to optimize expense, purchasing power from the grid as well as natural gas to fire the turbine. The throttle settings are changed up to three times per day to take advantage of fluctuating electricity and gas prices. This company has monitoring capability for the plant, but it is unknown exactly what hardware is installed to do so or its capability.

The computers in question, while normally “air gapped” run old versions of Windows that are no longer supported, presenting many software vulnerabilities that could be exploited to damage the plant or provide service outage.

The Central Utilities Plant has several targets and methods of breaking in to them. The power distribution switches on campus controlled from control room, presenting a situation that could unfold in a similar manner to the Ukraine power grid attack, albeit on a smaller scale. The turbine synchronization is controlled from the control room, which allows the same sort of control that was exploited in the Aurora demonstration, destroying a generator, although protection relays are present to prevent these sorts of faults. The steam and chilled water valves are remotely controlled from the control room, so a situation similar to the Turkish pipeline, minus the flammable mixture in the pipes, could be orchestrated. Most all of the hardware is either remotely monitored or monitored by an outside company. Anything that allows communication in this manner may be coopted to cause mischief or worse.

The security of such a facility is also vulnerable to human error. In some studies, it was discovered that files containing movies had been transferred to computers in the control room of a plant. They were presumably brought in on a USB drive and connected to a computer that is “air gapped” from the internet, meaning that it does not have network connectivity. So, even presumably “air gapped” facilities can be vulnerable to inevitable human errors.

A. Potential for Catastrophic Cyber Attack

In typical facilities, it is expected that mechanical components (e.g., pumps) will eventually experience failures. So, various approaches are used to mitigate the impact, such as extra capacity, redundant equipment, and/or backups.

But these approaches are largely based on the notion of independence of mechanical failures. That is, the probability of a high-quality pump failing is small, but the probability of two failing at the same is extremely small, etc.

But, that independence does not apply to a cyber attack that damages multiple components at the same time as easily as it damages one. As illustrated earlier, recovery from such physical damage can take a long time, which could lead to a catastrophic large-scale and long-term disruption to energy delivery.

VI. Small-Scale Demonstration of Vulnerability of Variable Frequency Drive

A variable frequency drive (VFD) is used to drive an electric machine at a variable speed. Applications usually include pumps and fans, where load is throttled by changing the shaft speed driving the equipment. Such devices have become ubiquitous in industrial environments, driving a majority of large motor loads.

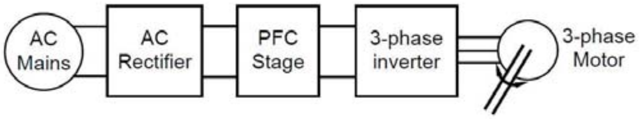


Fig. 9: Block representation of Variable Frequency Drive

A VFD consists of two main functional blocks, as shown in Fig. 9. There is a rectification stage, which takes alternating current (AC) power and turns it in to direct current (DC) power. This is usually a diode bridge, or in some cases, an active rectifier where controllable switches are used to improve performance. An inverter stage then turns DC back to AC, but at a different frequency and voltage than the original. This usually consists of a series of switches that are driven with a variable duty cycle to produce the proper output waveform. This output waveform is scaled to properly drive the attached motor. Various schemes exist to drive machines. A common one is a simple volts/Hz scaling, where the voltage of the AC waveform is scaled with the frequency. As the motor spins faster, the voltage required to drive it increases proportionally, keeping the flux inside the machine constant.

Other, more complicated schemes model various parameters inside the motor and attempt to control them directly. Vector control is a popular scheme.

Sitting between the two stages is an energy storage element. This consists of capacitors that store charge at an intermediate DC voltage to provide power to the driven motor. They are referred to as DC link capacitors. These capacitors are sized such that their voltage does not change appreciably throughout a single cycle. Given that power coming in from the rectifier is at comparatively low frequency, these devices are usually quite large and store large amounts of energy.

A power factor correction stage is often placed between the rectifier and energy storage elements. Its function is to cause power to be drawn at a power factor close to 1. Power factor is a measure of offset between the voltage and current waveforms drawn from the source. At a power factor of 1, the voltage and current are in phase. If the two are not in phase, the load draws reactive power, which does no real work, but is still charged for by the utility. Electric machines run at light load (reduced throttle) often draw significant reactive power, increasing their running costs

A. Variable Frequency Drive Test Kit

Shown in Fig. 10 is a Texas Instruments High Voltage Motor Development Kit. This is a unit built around TI's C2000 motor control chip and includes all of the hardware necessary to evaluate its function in driving a machine. In the lab, it is used to build custom motor drives. For our purposes in this project, it is a complete VFD with the added benefit of being supplied with source code with which we are immediately familiar. Such kits are sold with the idea that the control chip will be easily evaluated by a company's engineers and in turn used in their product lines.

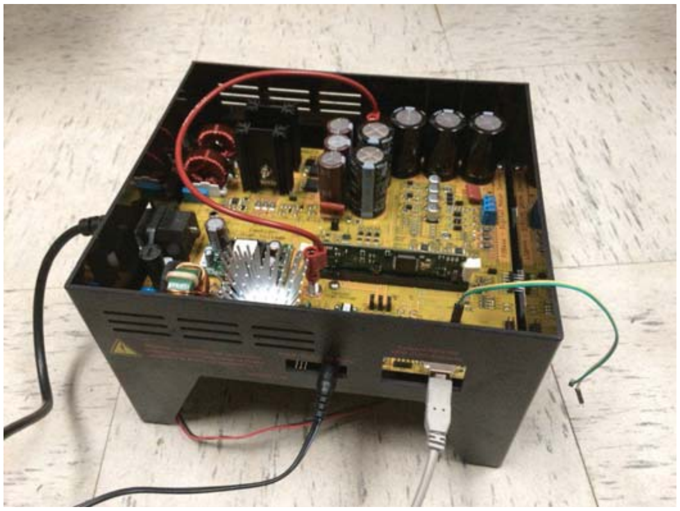


Fig. 10: Texas Instruments High Voltage 1 HP Motor Control Development Kit

Fig. 11 shows the block diagram of the TI motor driver. We can see the two main functional blocks mentioned above. The left side shows the AC mains (Vac) feeding a diode rectifier. On the middle right, we see a box labeled, "PWM" that contains the switches that comprise the inverter. In between, we have the power factor correction stage (PFC) as well as storage capacitors attached to the DC bus.

The immediately interesting aspect of this layout, from a cybersecurity perspective, which is shared by many VFDs used in industrial environments, is the power factor correction stage combined with the DC link capacitors. The power factor correction stage consists of two boost converters that operate out-of-phase with one another. By turning them on and off at opposite times, they draw power at near unity power factor. Boost converters are usually used in battery-powered electronics to boost the voltage from the battery level to that required by the device. They are also used in devices like flashes for cameras to create voltages high enough to fire a flash, which can be in the hundreds of volts range, from a battery at single digit volts. In our case, we rectify 120 V AC, then pass it through the power factor correction stage which brings it up to the ~400 V DC bus. The DC bus is monitored, and the drive signals to the power factor correction stage are adjusted to keep the DC bus voltage in the proper range. The important aspect here is that a large energy storage device is kept in its proper range by software control.

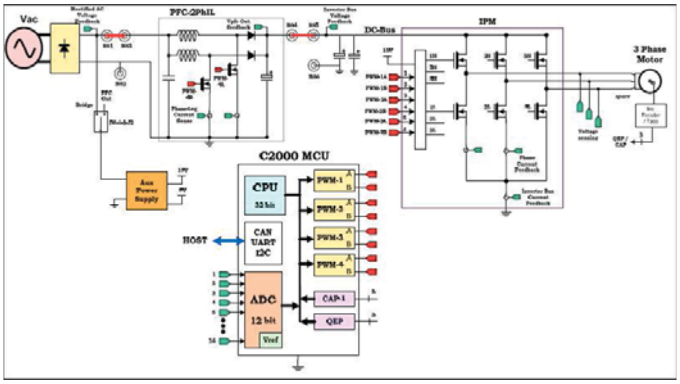


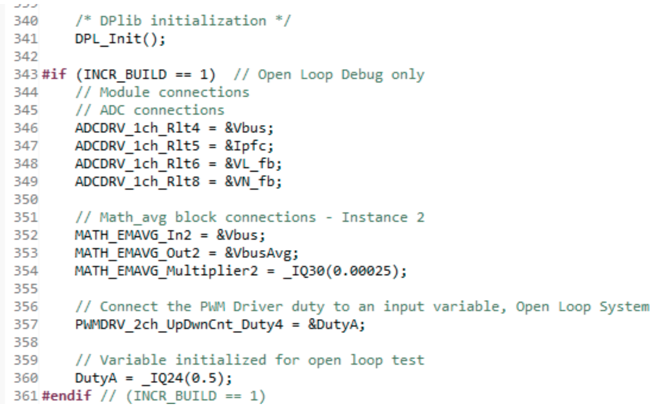
Fig. 11: Block Diagram of TI Motor Drive

A DC link capacitor stores a large amount of energy. In the lab, they are known to explode when they are exposed to excessive AC current, reverse biased, or exposed to voltages larger than their rating.

B. VFD vulnerability to malicious software

To demonstrate vulnerability to malicious software, the firmware in the VFD was modified to intentionally allow the voltage on the DC bus to run away.

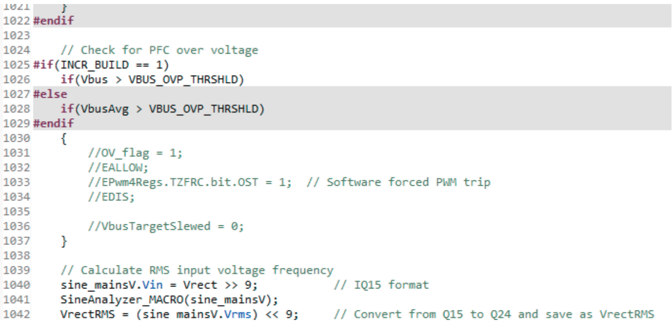
Fig. 12 and Fig. 13 show modifications performed to disable software control of the power factor correction stage and protection of the DC bus voltage. The converter is set up to run in an open-loop diagnostic mode, and then line 360 is modified to command a constant duty cycle, in this case .5.



```
340     /* DPlib initialization */
341     DPL_Init();
342
343 #if (INCR_BUILD == 1)  // Open Loop Debug only
344     // Module connections
345     // ADC connections
346     ADCDRV_1ch_Rlt4 = &Vbus;
347     ADCDRV_1ch_Rlt5 = &Ipfc;
348     ADCDRV_1ch_Rlt6 = &VL_fb;
349     ADCDRV_1ch_Rlt8 = &VN_fb;
350
351     // Math_avg block connections - Instance 2
352     MATH_EMAVG_In2 = &Vbus;
353     MATH_EMAVG_Out2 = &VbusAvg;
354     MATH_EMAVG_Multiplier2 = _IQ30(0.00025);
355
356     // Connect the PWM Driver duty to an input variable, Open Loop System
357     PWMDRV_2ch_UpDwnCnt_Duty4 = &DutyA;
358
359     // Variable initialized for open loop test
360     DutyA = _IQ24(0.5);
361 #endif // (INCR_BUILD == 1)
```

Fig. 12: Duty cycle modification on line 360

In Fig. 13, the procedures that protect the DC bus voltage are simply commented out. This prevents the unit from shutting down once the voltage rating is exceeded.



```
1021    }
1022 #endif
1023
1024    // Check for PFC over voltage
1025 #if(INCR_BUILD == 1)
1026    if(Vbus > VBUS_OVP_THRSHLD)
1027 #else
1028    if(VbusAvg > VBUS_OVP_THRSHLD)
1029 #endif
1030    {
1031        //OV_flag = 1;
1032        //EALLOW;
1033        //EPwm4Regs.TZFRC.bit.OST = 1;  // Software forced PWM trip
1034        //EDIS;
1035
1036        //VbusTargetSlewed = 0;
1037    }
1038
1039    // Calculate RMS input voltage frequency
1040    sine_mainsV.Vin = Vrect >> 9;           // IQ15 format
1041    SineAnalyzer_MACRO(sine_mainsV);
1042    VrectRMS = (sine mainsV.Vrms) << 9;     // Convert from Q15 to Q24 and save as VrectRMS
```

Fig. 13: Disabling of overvoltage protections (lines 1031-1036)

The result of these software tweaks is shown in Fig. 14. The oscilloscope is showing the drive signal to the power factor correction stage (PWM 4A from Fig. 11). This was performed to demonstrate control of the duty cycle feeding the power factor correction stage. Also seen in Fig. 14 are the capacitors on the DC bus. They are the cylindrical items in the drive on the far right of the Fig..

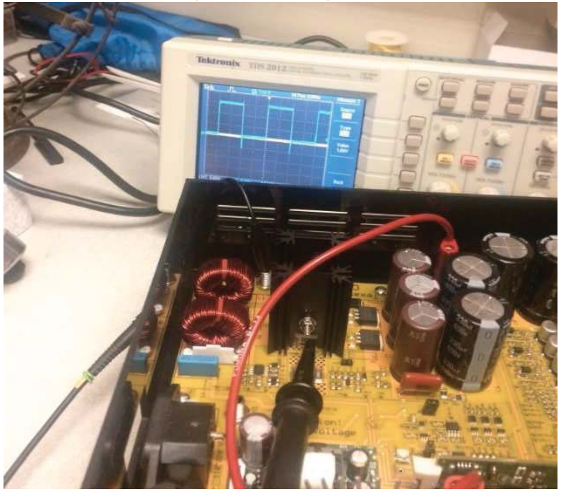


Fig. 14: Demonstration of Duty Cycle control on Power Factor Correction stage

The capacitors on the DC bus are rated to 450V. The DC bus is somewhat less than this to ensure a long component life. When run open-loop and with no load connected to it, the voltage on the output of a boost converter will rise without limit. In our case, we expect the capacitors to begin leaking current, eventually constraining voltage on the output of the boost converter far beyond their voltage rating. It will then be only a matter of time before the capacitors catastrophically fail, as the current leakage will heat the fluid inside until the point where the case bursts. If one of the capacitors shorts internally, it may cause further damage to the rest of the capacitors on the bus.

Fig. 15 shows the result of a small-scale test of this concept. The power factor correction stage was set to run open-loop, and the voltage protection shutdowns were disabled. Voltage on the bus rose to approximately 550 V, and the capacitors exploded one by one. While there was no violent explosion or damage to nearby structures, it did fill a large area with smoke. The DC bus in this case stores 200 Joules at rated voltage, or the energetic equivalent of approximately seven firecrackers [12].

Once all of the capacitors had exploded, voltage rose to the point where one of the switches in the converter failed, causing an internal short and blowing the input fuse on the VFD. In an industrial setting, this would have disabled any load attached to it, but only after significant damage had been done to the capacitors, the VFD, and possibly nearby equipment.

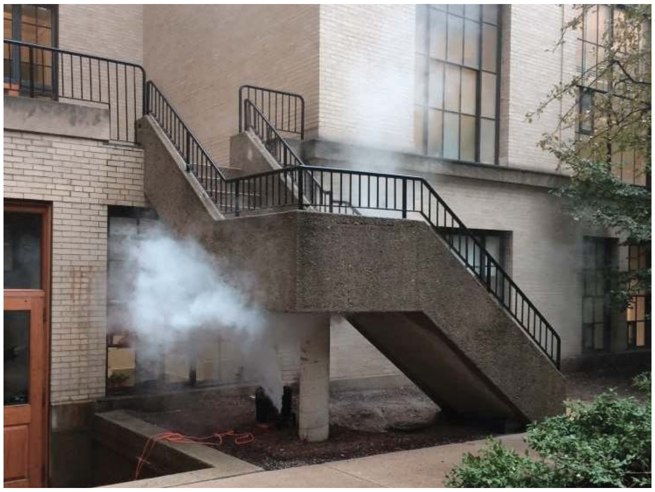


Fig. 15: Small Scale Test showing destruction of DC link capacitors

C. Larger scale vulnerability possibilities

Capacitors scale with output power of the drive. Shown in Fig. 16 is the DC link capacitor bank of a 100 HP drive. The white cylinders are capacitors, and the metal plates on the ends are the DC bus bars.

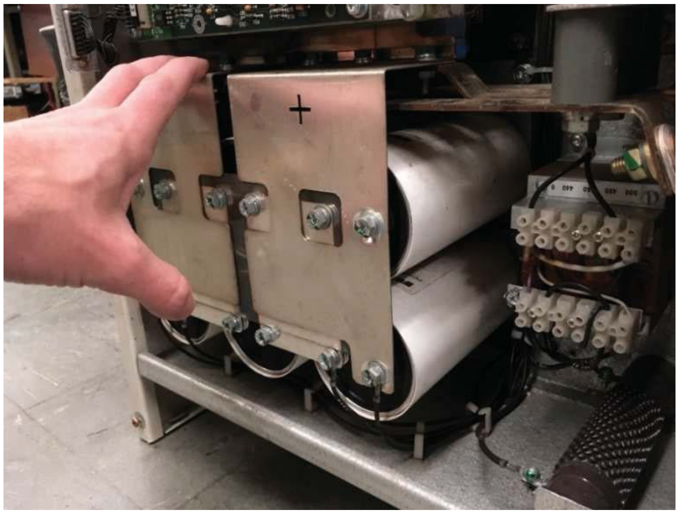


Fig. 16: DC Link Capacitors on 100 HP Inverter

The capacitors in the DC link are 7290 μF and rated to 280 V. If they were to explode in the same manner as the demonstration, they would release approximately 1700 Joules, or about 60 firecrackers [12].

In an industrial setting, VFDs may be much larger. In the MIT Central Utilities plant, there are several large VFDs driving chilled water pumps. Fig. 17 shows the electrical diagram of the central utilities plant, containing many several-hundred-horsepower VFDs.

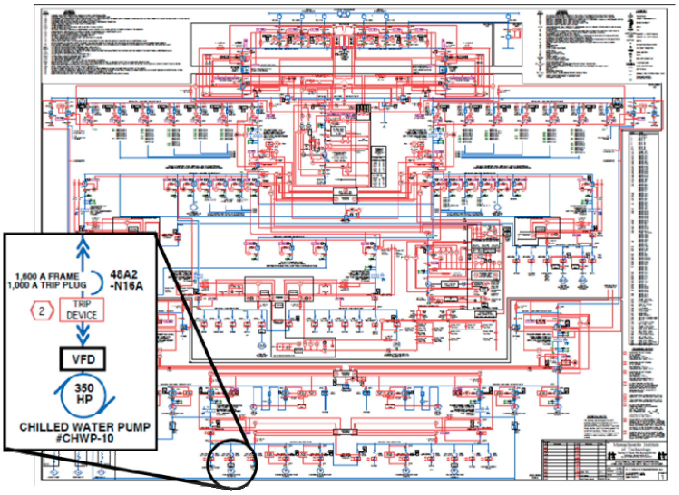


Fig. 17: Electrical diagram of MIT Central Utilities Plant showing 350 HP Chilled Water Pump

Fig. 18 shows a 500 horsepower VFD. The cabinet contains breakers and large cooling devices, but also very large energy storage capacitors on a DC bus that could be attacked in the same way as the capacitors in the 1 hp unit in the demonstration above.

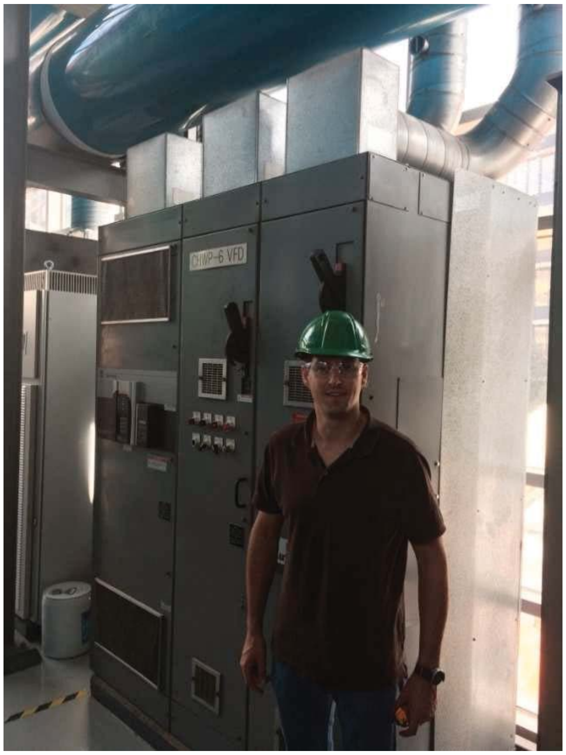


Fig. 18: Size comparison with 500 HP VFD

D. Cybersecurity vulnerabilities and prior VFD energy storage failure examples

Modern VFDs may be conFig.d and commissioned over a network connection. Firmware may be remotely pushed to the device over the network as well. Such capabilities may be readily exploited by malicious actors to cause damage to the VFD itself or the machinery connected to it.

Many attack surfaces exist for VFDs in industrial settings. Features may be used by a malicious hacker to damage the hardware attached to the drive. One such feature is the ability to skip certain frequencies when starting up or running. This is done to prevent excitation of resonances in the mechanical systems the drives are controlling. This feature, being a user programmable setting, may be queried from the network on many drives. It is then a simple matter to command the drive to operate at the damaging frequency [13] [14].

As mentioned earlier, there are other ways to cause an energy storage capacitor to fail. Fig. 19 and Fig. 20 show the result of a capacitor failure in the harmonic filter of the cruise ship Queen Mary II. In this case, the dielectric oil inside the capacitor evaporated over time, eventually allowing an arc to form inside the capacitor. The heat generated from the flashover caused in increase in pressure, which ruptured the case, spraying out the remaining oil, which presented a conduction path to the bus bars. This caused a major arc flash event, destroying the compartment and even blowing out the door to the compartment (Fig. 20).

This sort of damage can be caused by many factors, including excessive harmonic content in the output of the motor drives. This is something that could be intentionally caused by very subtle, unnoticeable, changes to the way in which the output stage of the drive operates, causing very large amounts of damage at unpredictable times. In this case, the damage to one capacitor did not disable the ship, but simultaneously damaging several harmonic filter capacitors on the main propulsion motors could strand the ship. This has obvious military implications as well with the move to electric propulsion.

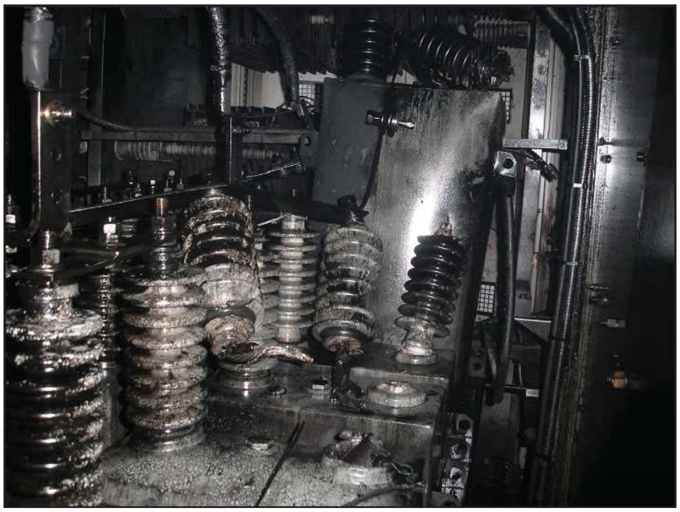


Fig. 19: Capacitor Explosion on Queen Mary II REF SB4-10

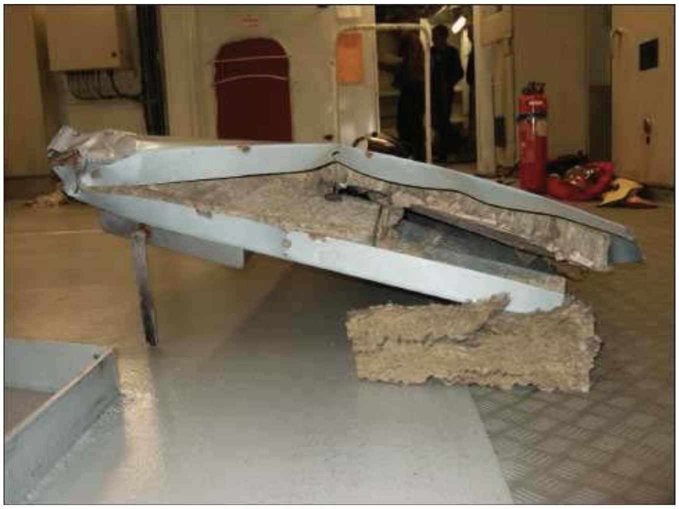


Fig. 20: Steel Door from Harmonic Filter Capacitor bank on Queen Mary II REF SB4-10

An example of unintentional physical damage caused by a VFD is shown in Fig. 21. This is the guard surrounding the coupling on an 18000 hp pump owned by ExxonMobil. In this case, a speed feedback signal was improperly wired around a filter, creating an unfiltered feedback path that caused a system resonance at the natural frequency of the coupling. Resulting torque pulsations quickly destroyed the coupling, requiring repair and research to determine the cause of the failure. While there was expensive damage done to the machine, down time was likely the real cost. Stuxnet was an example of exactly the same phenomenon, except implemented intentionally as an attack.

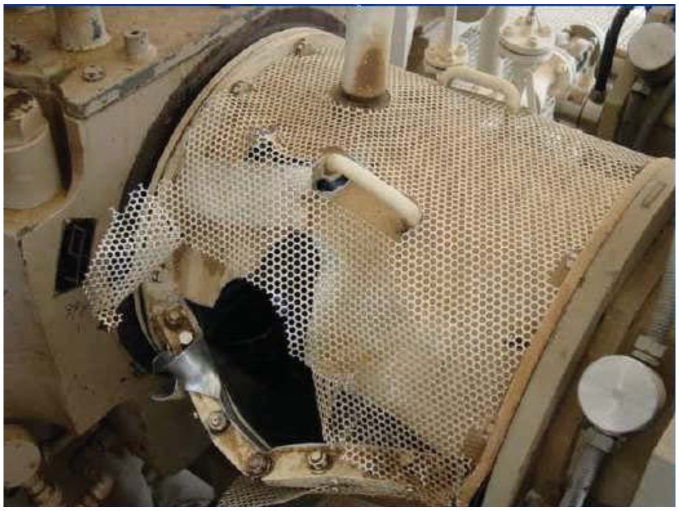


Fig. 21: VFD-induced Coupling Failure on 18000 HP LPG Compressor [15]

VII. Conclusion

Electronics with energy storage components or that control physical systems are capable of a wide variety of physical damage should the software that controls them be improperly conFig.d or maliciously attacked. This phenomenon is immediately obvious to anyone who has spent time in the lab building such devices, as mistakes are often righted with a fire extinguisher. Electrical energy storage devices in a variety of systems contain sufficient energy to cause damage. The small demonstration presented here scales to potentially cause catastrophic damage in an industrial setting, potentially endangering personnel as well as an industrial process. The techniques used here are adaptable to cause other modes of physical damage that are seen in literature.

VIII. Acknowledgment and Disclaimer

This material is based, in part, upon research supported by the Department of Energy under Award Number DE-OE0000780 and a seed grant from the MIT Energy Initiative (MITei).

Disclaimer: Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

IX. References

[1] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," 26 September 2007. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/.

[2] M. J. Thompson, Fundamentals and Advancements in Generator Synchronizing Systems.

[3] M. T. Coyle, "USNRC 50-461: Licensee Event Report (LER) No. 2000-002-00," 2000. [Online]. Available: https://www.nrc.gov/docs/ML0036/ML003698812.pdf.

[4] L. Scott Anderson and Lawrence C. Gross, Jr., "Avoid Generator and System Damage Due to a Slow Synchronizing Breaker," 24th Annual Western Protective Relay Conference, October 1997.

[5] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," 3 March 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[6] "Ukranian National Electric Grid," [Online]. Available: http://www.geni.org/globalenergy/library/national_energy_grid/ukraine/ukrainiannationalelectricitygrid.shtml.

[7] "Analysis of the CyberAttack on the Ukranian Power Grid," 18 March 2016. [Online]. Available: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[8] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar," 10 December 2014. [Online]. Available: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[9] H. English, "Turkish official confirms BTC pipeline blast is a terrorist act," 14 August 2008. [Online]. Available: http://www.hurriyet.com.tr/turkish-official-confirms-btc-pipeline-blast-is-a-terrorist-act-9660409.

[10] D. Kushner, "The Real Story of Stuxnet," 26 February 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[11] K. Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," 3 November 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[12] J. Zimbelman, "How Big is 'BIG!'?: Comparing Forms of Energy Release,"[Online]. Available: http://www.si.edu/Content/consortia/Zimbelman_presentation.pdf.

[13] K. Zetter, "There's a Scary Easy Way for Hackers to Remotely Attack Industrial Motors," 13 January 2016. [Online]. Available: http://www.slate.com/blogs/future_tense/2016/01/13/vulnerability_lets_hackers_burn_industrial_motors.html.

[14] "Variable Frequency Drives - VFD Vulnerabilities," 14 March 2016. [Online]. Available: http://www.alphaguardian.net/variable-frequency-drive-vfd-vulnerabilities/.

[15] J. Kocur, in Proceedings of the 37th Turbomachinery Symposium.

[16] "Iran's gas flow to Turkey halted after pipeline blast – official," [Online]. Available: https://www.rt.com/news/364502-turkey-gas-explosion-iran/.

X. Biographies

Matthew G. Angle is a Postdoc in the Department of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. He received his SB(2007), MEng (2011), and Ph.D. (2016) degrees in Electrical Engineering from MIT.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technology and a Professor of Engineering Systems at the Massachusetts Institute of Technology. He has been an MIT faculty member since 1972. He has served as the head of MIT's Information Technologies Group in the MIT Sloan School of Management for more than twenty years. Currently he is the Director of MITs Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)3. He is the author or co-author of over 350 books, articles, or reports including the classic textbook on *Operating Systems,* plus several patents. His current research interests include cybersecurity, information integration technologies, semantic web, software project management, internet applications, and the strategic use of information technology. Madnick has been active in industry, as a key designer and developer of projects such as IBM's VM/370 operating system and Lockheed's DIALOG information retrieval system. He has served as a consultant to major corporations, including IBM, AT&T, and Citicorp. He has also been the founder or co-founder of five high-tech firms, and currently operates a hotel in the 14th century Langley Castle in England. Madnick holds an SB in electrical engineering, an SM in management, and a PhD in computer science from MIT.

James L. Kirtley Jr. is Professor of Electrical Engineering at the Massachusetts Institute of Technology. He has also worked for General Electric, Large Steam Turbine Generator Department, as an Electrical Engineer, for Satcon Technology Corporation as Vice President and General Manager of the Tech Center and as Chief Scientist, and was Gastdozent at the Swiss Federal Institute of Technology. He continues as a Director for Satcon. Dr. Kirtley attended MIT as an undergraduate and received the degree of Ph.D. from MIT in 1971. Dr. Kirtley is a specialist in electric machinery and electric power systems. He served as Editor in Chief of the IEEE Transactions on Energy Conversion from 1998 to 2006 and continues to serve as Editor for that journal and as a member of the Editorial Board of the journal Electric Power Components and Systems. Dr. Kirtley was made a Fellow of IEEE in 1990. He was awarded the IEEE Third Millenium medal in 2000 and the Nikola Tesla prize in 2002. Dr. Kirtley was elected to the United States National Academy of Engineering in 2007. He is a Registered Professional Engineer in Massachusetts.