CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Research Activity
Fact Sheet

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

Website: http://cred-c.org/researchactivity/preventotpd

Researchers (MIT): Stuart Madnick, James Kirtley, Matt Angle, Michael Siegel, Mohammad Jalali, Shaharyar Khan, Taylor Hartley Andrews, Nabil Sayfayn

Industry Collaboration:

- **Current collaborators:** MIT Co-Generation Facility, Engie, ExxonMobil, Engie, Schneider Electric, Hitachi
- We will be seeking additional collaborators from the companies who expressed strong interest at CREDC Industry Workshop.

Description of research activity: Most attacks on Energy Delivery Systems (EDS) 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 cases like these where there is no physical damage, recovery is largely a matter of restarting computers and resetting breakers. But, if the Operational Technology equipment, especially large, costly, and critical customized equipment, is physically damaged, recovery can take weeks or even months. An example of this kind of attack was to the centrifuges of the Iranian uranium enrichment facility.

It is important that we identify and anticipate such dangers in advance – which is the goal of this research. Our research uses a system-theoretic approach to develop an analysis tool that OT operators can use to identify vulnerable EDS targets and failure scenarios and develop enhancements to the hierarchical control structure to minimize possible physical damage. The goal is to eliminate or restrict hazard conditions that can lead to a dramatic loss, and implement effective countermeasures during design and/or operation for OT operators.

To illustrate the importance and significance of this research, an analysis of the MIT Cogeneration Facility has started. Using our physical property analysis of the Operational Technology being used, a serious vulnerability has been uncovered related to Variable Frequency Drives (VFDs) and their associated capacitors. As shown in Figure 1, VFDs are used extensively at the MIT Cogeneration facility and are commonly found in EDS.

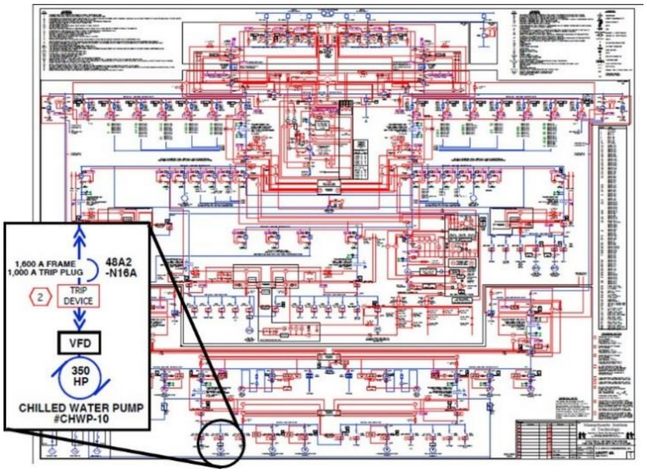


Figure 1. MIT Cogeneration facility usage of Variable Frequency Drives (VFD)

It is important to realize that increasingly, to provide maximum flexibility, VFDs are operated under software/firmware control. Even the safety features are under software control. So, a successful cyber attack could cause major harm. To demonstrate this vulnerability, we modified only a few lines of firmware (similar to what was done to other devices during the Ukrainian attack) on a small VFD test kit which resulted in an explosion of the capacitors, as shown in Figure 2.

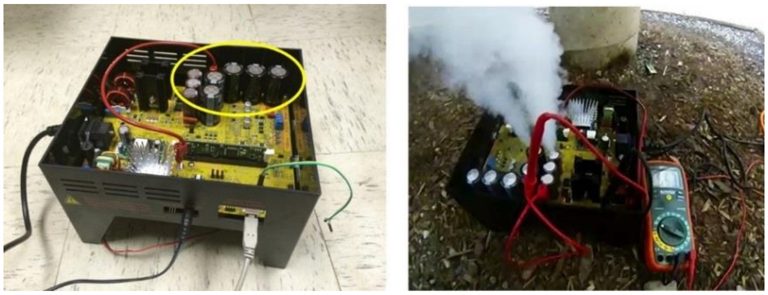
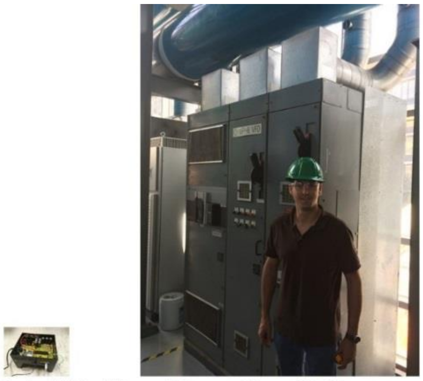


Figure 2. (Left) Small VFD test kit, (Right) Explosion of VFD test kit caused by minor firmware changes

In studying the analysis of the VFD vulnerabilities at the MIT Cogeneration Facility, the magnitude of the threat is illustrated by comparing the size of the VFD test kit with the actual VFDs used, as shown in Figure 3.



Student VFD test kit experiment

VFD controlling a 400 HP motor

Figure 3. (Left) Small 1HP VFD test kit, (Right) VFD controlling a 400 HP motor

A successful attack, similar to that demonstrated in Figure 2, would likely not only physically damage the VFD but also nearby equipment. Our proposed PreventOTPhysDamage tool can help avoid such a situation.

The tool, with extensive graphical and easy-to-use interface, will be used by OT operators. It will have several capabilities:

(1) It will guide the OT operators to identify critical cybersecurity vulnerabilities that have potential for significant OT physical damage.
(2) For each such situation, it will help to define the hierarchical control structure, including the processes, the controllers (which might be mechanical, electronic, and/or human), and the sensors and actuators that are intended to provide cybersecurity protection.
(3) It will evaluate the effectiveness of the control mechanisms, focusing on Goal, Action Condition, Observability Condition, and Model Condition.
(4) It will specifically highlight dangers possible due to failure of physical/operational controls, physical failures, dysfunctional interactions/communications, and/or unhandled external disturbances.
(5) The tool will provide recommendations for improving the cybersecurity of the vulnerability and provide a risk assessment.

As an initial test case, we are progressing at the MIT Cogeneration facility with our systematic systems-theoretic analysis of the control structures and OT operator procedures and controls needed to mitigate catastrophic damage.

Assessment of Originality and Relevance of Proposed Research
Since we do not want to duplicate research already done nor research that would have no value, we have extensively investigated the originality of our proposed research and its likely relevancy to the EDS industry.

We have done this in multiple ways.

First, we studied the existing published literature and could find no papers that address the issues that we are investigating and that we presented at the CREDC Industry Workshop.

But, since literature can be scattered and often incomplete, we have reached out to hundreds of experts in the Industrial Control Systems (ICS) industry, and especially the EDS industry.

We accomplished this is multiple ways (in each case, asking “Have they seen such research published anywhere? Is this important?”):

(1) We presented our preliminary results at the ARC Forum, an annual gathering of over 300 professionals in ICS, and especially EDS, in February 2017. From the podium, we asked our questions. Not surprisingly, everything thought that preventing physical damage was important. No one identified any prior published work.
(2) We presented the same work, in poster form, at the CREDC Industry Workshop and got similar responses. In that case, we were able to speak to people one-on-one. In fact, six of the industry representatives requested that we contact them to follow up further. This included people from ABB and PNNL, and others who were very familiar with the state-of-the-art.
(3) Furthermore, we reached out to our collaborators at places like ExxonMobil, Schneider Electric, Engie, etc. and sent them a draft of the paper we are writing, based on the CREDC poster. We asked them to ask around their organizations the same questions, and got the same responses: They agreed that our report was reasonable and accurate and that they had not seen any such findings published. We even communicated with an internationally known cybersecurity organization (who requested anonymity) that has a group specializing on ICS, who also agreed.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?

- Assess and Monitor Risk
- Develop and Implement New Protective Measures to Reduce Risk

Summary of EDS gap analysis: To date, most attacks on Energy Delivery Systems (EDS) 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 cases like these where there is no physical damage, recovery is largely a matter of restarting computers and resetting breakers. But, if the Operational Technology equipment, especially large, costly, and critical customized equipment, is physically damaged, recovery can take weeks or even months. An example of this kind of attack was to the centrifuges of the Iranian uranium enrichment facility.

The Aurora Vulnerability research demonstrated this danger to generators and alerted utilities to introduce procedures to mitigate such an attack. It is important that we identify and anticipate such dangers in advance. As most informed experts have noted, although we can make it more difficult for an attacker by air-gapping and other means, “prevention (of cyber attack) is futile.” So, we need to take steps to anticipate and mitigate the physical damage that can be accomplished by a cyber attack – which is the goal of this research.

Our research uses a system-theoretic approach to develop an analysis tool that OT operators can use to identify vulnerable EDS targets and failure scenarios and develop enhancements to the hierarchical control structure to minimize possible physical damage. The goal is to eliminate or restrict hazard conditions that can lead to a dramatic loss, and implement effective countermeasures during design and/or operation for OT operators.

Full EDS gap analysis:

Motivation: To date, most attacks on Energy Delivery Systems (EDS) have either targeted the IT infrastructure (e.g., the Aramco Shamoo attack) or circuit breakers of the Operational Technology (e.g., the Ukraine attack [5], [11], [13]. In cases like these where there is no physical damage, recovery is largely a matter of restarting computers and resetting breakers, which can be done quickly. But, if the Operational Technology equipment, especially large, costly, and critical customized equipment, is physically damaged, recovery can take weeks or even months. An example of this kind of attack was to the centrifuges of the Iranian uranium enrichment facility [7], [12].

The Aurora Vulnerability research [6], [8], [10], conducted by the Idaho National Laboratory, demonstrated this danger to generators and alerted utilities to introduce procedures to mitigate such an attack.

It is important that we identify and anticipate such dangers in advance. As most informed experts have noted, although we can make it more difficult for an attacker by air-gapping and other means, “prevention (of cyber attack) is futile.” So, we need to take steps to anticipate and mitigate the *physical* damage that can be accomplished by a cyber attack – which is the goal of this research.

Approach: Our research uses a system-theoretic approach [1] to develop an analysis tool that OT operators can use to identify vulnerable EDS targets and failure scenarios and develop enhancements to the hierarchical control structure to minimize possible physical damage. The goal is to eliminate or restrict hazard conditions that can lead to a loss, and implement effective countermeasures during design and/or operation to recommend mitigation for OT operators.

Relationship to Road Map: This research addresses:

- Assess and Monitor Risk
- Develop and Implement New Protective Measures to Reduce Risk

Relationship to NESCOR: This research relates to many NESCOR scenarios, the closest one being: “The DER owner fails to change the default password or not set a password for the DER system user interface. A threat agent (inept installer, hacker, or industrial spy) gets access through the user interface and changes the DER settings so that it does not trip off upon low voltage (anti-islanding protection), but continues to provide power during a power system fault; Impact: DER system suffers physical damage due to feeding into a fault.”

The proposed research actually go beyond this scenario by considering situations where much more serious physical damage could be done and which could be initiated through a broader variety of cyber-attacks.

Relationship to ES-C2M2: ES-C2M2 defines 10 different domains and for each domain it defines three maturity levels. This proposal relates to many domains, though the closest would be the domain: "threat and vulnerability management" which comprises three objectives: identify and response to threats, reduce cybersecurity vulnerabilities, management activities. ES-C2M2 presents examples such: "when reducing cybersecurity vulnerabilities, ...identify the potential impacts of known software vulnerabilities, this allows the organization to prioritize reduction activities according to the importance of the vulnerabilities". One of the primary focuses of this proposal is to identify some important but unknown vulnerabilities. In addition, since each scenario describes the failure and the impact, we can go through the scenario to identify the attack graph for the EDS sector.

Relationship to current practices and offerings by consulting companies: We took two routes to best understand the current practices and offering by consulting companies: (1) We talked with many cybersecurity experts in the EDS industry – as explained in the section “Assessment of Originality and Relevance of Proposed Research” and (2) we researched the literature and contacted companies that specialize in providing related services – as explained in the Appendix “Review of Literature on Risk Assessment of OT Systems and Related Companies and How they compare with MIT’s Prevent OT Physical Damage CREDC proposal.” The appendix includes materials collected from some of these companies.

Our conclusion is (summarized from the Appendix):

The “Prevent OT Physical Damage” CREDC proposal is quite different from all of these. It is looking at individual components in an ICS system and identifying not just methods of intrusion, but methods of destruction (which is clearly an important distinction – and especially and uniquely important in the EDS world.) We're not concerned (at least in terms of priority) with how the systems are accessed, but more with what can be done once the network defenses are defeated, which any network security person will tell you, can happen via a variety of methods, or even leveraging required functionality for malicious purposes. Our tool would make recommendations about how to prevent system or plant-wide damage with non-user-adjustable devices once the hardware is installed**.**

Fundamentally, the companies studied and the risk assessment methods identified in the papers reviewed assume finite and indiscriminate disruption. They fail to take in to account the ability to turn a known system with a high degree of correlation into a smoking hole in the ground, and the ease at which this can be done with basic knowledge of how the systems works once network access has been granted.

We're not looking at causing undesired action on the networks, but instead leveraging capabilities that are necessary for their function to inflict serious destructive harm.

Bibliography:

[1] Asare, Philip, Lach, Stankovic John,, FSTPA-I: A Formal Approach to Hazard Identification via System Theoretic Process Analysis, Proceedings of ICCPS April 8–11, 2013, Philadelphia, PA. <https://www.cs.virginia.edu/~stankovic/psfiles/Asare-et-al-FSTPA-I-ICCPS13.pdf>

[2] Coyle, Michael T. "USNRC 50-461: Licensee Event Report (LER) No. 2000-002-00." 2000.

[3] English, Hurriyet. Turkish official confirms BTC pipeline blast is a terrorist act. 14 August 2008. <http://www.hurriyet.com.tr/turkish-official-confirms-btc-pipeline-blast-is-a-terrorist-act-9660409>.

[4] Iran's gas flow to Turkey halted after pipeline blast – official. n.d. < https://www.rt.com/news/364502-turkey-gas-explosion-iran/>.

[5] ISAC, Analysis of the CyberAttack on the Ukranian Power Grid. 18 March 2016. <http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf>.

[6] Kocur, John. Proceedings of the 37th Turbomachinery Symposium. n.d.

[7] Kushner, David. The Real Story of Stuxnet. 26 February 2013. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

[8] Lawrence C. Gross, Jr. and L. Scott Anderson. "Avoid Generator and System Damage Due to a Slow Synchronizing Breaker." n.d.

[9] Meserve, Jeanne. Sources: Staged cyber attack reveals vulnerability in power grid. 26 September 2007. <http://www.cnn.com/2007/US/09/26/power.at.risk/>.

[10] Thompson, Michael J. Fundamentals and Advancements in Generator Synchronizing Systems. n.d.

[11] Ukranian National Electric Grid. n.d. <http://www.geni.org/globalenergy/library/national_energy_grid/ukraine/ukrainiannationalelectricitygrid.shtml>.

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

[13] —. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. 3 March 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

[14] Zimbelman, Jim. How Big is 'BIG!'?: Comparing Forms of Energy Release. n.d. <http://www.si.edu/Content/consortia/Zimbelman_presentation.pdf>.