

Physical Security Challenges and Responses for High Voltage Transformers

JAMES MC IVER – SIEMENS TRANSFORMERS USA
4601 SIX FORKS ROAD
Raleigh NC 27609
702-241-0157/no FAX
JAMES.MCIVER@SIEMENS.COM

INTRODUCTION

Transmission substations and power transformers have historically been designed and operated with redundancies in mind. This often includes redundant circuits, system spares, and/or the ability to redirect power flows after the loss of a single power transformer. Transmission system planners and operators are extremely comfortable with this “N-1” contingency approach, where elements of the transmission system are removed in operational studies to assure that the system will continue to operate as expected. The result of this advance planning may lead to development of system redundancies and operational re-configurations, such that loss of network elements can be tolerated without the occurrence of outages or system collapses.

However, in light of recent experience, the North American transmission system may also be susceptible during increasing occurrences of major disruptive events. These additional events can be loosely grouped under the heading of “common-mode failures”, rather than previously anticipated N-1 losses. Major weather events (including solar storms, hurricanes, storm surges, and tornadoes) as well as manmade threats (such as cyber-security risks and vandalism) may disrupt a large portion of a transmission system. These major events may require different responses than those anticipated for loss of a single transmission asset.

There is growing regulatory concern about power system resiliency in the face of these more wide-spread and common-mode threats. As a result, NERC has issued CIP-014, which requires transmission asset owners to develop plans to enhance the physical security of their critical substations. Responses to the CIP-014 mandate may take the form of risk minimization, enhanced replacement capabilities or the use of “hardened” transmission assets. It falls upon the transmission owner to derive a comprehensive approach to security improvements, using any or all of these philosophies.

This paper will discuss both a formalized approach to risk assessment and some steps that can be taken to improve the security of power transformers. Several “resilient transformer” approaches have been developed by Siemens in cooperation with participating transmission owners. It will be shown that increased interaction between asset owner and manufacturer can achieve enhanced physical security applying a modular architecture .

RESILIENCY ASSESSMENT

The design, installation and operation of new large power transformers (LPTs) can be modified in order to achieve enhanced physical security, but effective solutions require more than just hardware modifications. Increased interaction is needed between the asset owner and manufacturer in order to ensure that credible security concerns are addressed at the time of design and manufacture. This process can be described in the following five steps:

- 1) Threat assessment and expected resiliency planning in face of a defined threat
- 2) Desired operational performance of affected substation and power transformer
- 3) New options for delivery, storage and operation
- 4) Identification of necessary changes in technology, operation and/or logistics
- 5) Production of modified power transformer within the newly defined specifications

Threat Definition

Because industry and regulatory concerns are still developing with regard to new and wide-ranging system threats, it is vital that threat definition and assessment become the first step in resiliency analysis. In the electric power industry, many parties are engaging in discussions of “what can be done” without first developing a clear picture of the threats and solutions which need the highest priority. There is a large array of threats to consider, and each transmission asset owner will be subjected to a different mix of these threats.

Before threat responses or equipment modifications are undertaken, it is important for the asset owner to methodically determine those threats applicable to his security scenario. As an example of threat assessment for an individual asset owner, consider the range of threats that need to be considered:

- Cyber-security
- Natural disasters (e.g. weather-induced)
 - storm surge
 - tornadoes/hurricanes
- solar storms
- Physical impacts

Each of these threats may be theoretically possible, but it would be impossible and foolhardy to try and address all possible threats simultaneously. Rather, the asset owner must consider system concerns, geographical location and functional limitations during threat impact. This will help to prioritize threats and highlight those events which most urgently require a response. For example, one asset owner may be exposed to weather threats such as storm surges or hurricanes, while another may need to focus on threats created by physical impacts.

Threat Assessment

Methodical threat definition will naturally lead to a determination of those power system assets which are most vulnerable to identified threats. The threat assessment stage will help the asset owner to define which substation equipment is more likely to be affected by high priority threats and what impacts upon the bulk power system may be expected.

For purposes of this paper, cybersecurity threats are not considered. Various physical security challenges affecting overall transmission substation installations are discussed by other authors. Therefore, this paper will concentrate on the physical security of LPTs. It is generally considered that LPT assets have the greatest vulnerability to physical threats, both because of their size and particularly because of the extended replacement and repair time required when LPTs are damaged or destroyed.

LPTs will in general benefit from overall substation security improvements, such as added walls, access barriers/gates/guards, or improved lighting/cameras/motion detection. However, analysis of physical security threats will often show that LPTs remain vulnerable to damage or destruction, even if the substation itself has not been penetrated.

Due to the wide diversity of ratings, criticality and location, the consideration of LPTs may often lead to threat assessment on a case-by-case basis. It is important for the asset owner at this stage of the analysis to clearly determine the following:

Is LPT vulnerability considered as asset-specific, site-specific or system-wide?

It is likely at this early stage of industry-wide assessment that a limited number of critical LPTs will be analyzed in detail. However, as the issue of physical security becomes more embedded in industry practices, it can be foreseen that more standardized protection and recovery responses will be developed to improve system-wide vulnerabilities.

Siemens is currently engaged in providing asset-specific or site-specific solutions to a variety of asset owners. While CIP-014 is in its early stages of implementation, there is a natural tendency to apply solutions for asset owners' specific and critical physical security scenarios. However, we are also encouraging the possibilities of broader physical security solutions that can be implemented on an industry-wide basis. This is in direct response to the interests and mandates which are originating from regulators for a more comprehensive approach to physical security. The outcome of threat definition and assessment will be a clear understanding ⁽¹⁾:

- What needs to be protected?
- Who/What are the threats?
- What are the system vulnerabilities to these threats?
- What are the implications if these assets were damaged or lost?

IDENTIFY PROTECTION AND RECOVERY ACTIONS

What can be done to minimize LPT exposure to defined loss or damage scenarios?

Following the use of risk assessment methodology (as suggested by CIP-014 and described above), the next step to minimize LPT exposure is an organized and comprehensive process which defines effective recovery and protection parameters for each individual asset owner.

In the case of physical threats to LPTs, a basic protection philosophy needs to be established:

Is multi-stage protection appropriate for the identified threat scenario?

Note that implementation of multiple protection levels is quite common in the case of relay protection, cyber security, or bulk power generation reliability. However, LPT protection and availability is generally limited to implementation of the N-1 planning criterion. This means that loss of an individual transformer is not necessarily mitigated – rather, the loss is accommodated through the use of redundant system capacity or available equipment spares. In the case of the industry’s evolving understanding of physical security, exclusive reliance on N-1 planning may not be enough.

Assessment of LPT physical threats may very well lead to use of a “protection-in-depth” philosophy. In addition to the physical security substation improvements mentioned above, the LPT may need to be “hardened” and have its own physical protection. Also, there can be considerable benefit to implementing an improved LPT sparing philosophy as the final line of defense.

Physical & Electrical Protection

Protection strategy can encompass any actions and design elements aimed at protecting transformers from natural disasters and physical impacts. For transformer protection-in-depth, this will require features beyond those security measures discussed above for the substation site.

In the Siemens comprehensive concept for transformer resiliency, this means a focus on both physical threats (such as vandalism or gunfire attacks) plus withstand of DC-incursions into the ac power system in the case of solar storms and geomagnetically-induced currents (GIC).

The Siemens resilience concept offers, among other features, a bullet-resistant design, which adds a protective surface around the transformer tank. This material provides protective plate to protect the main transformer tank from possible gunfire attacks and offers greater ballistic protection than a concrete block wall. It is mounted onto the main tank with brackets and no additional civil (foundation) work is required, as would be the

case for a concrete wall. Hatches and vertical extensions can be provided to permit access to externally mounted accessories and conservator tanks. The vertical extensions presented by high voltage bushings will remain exposed, but it is recommended that non-porcelain RIP or RIS bushings should be used for enhanced survivability and safety in the case of physical attack. In addition to their increased physical withstand, these newer bushing types do not contain oil and therefore no fire or explosion will occur.

In the case of possible damage due to solar-storms, Siemens transformer designs can be analyzed for the owner's expected levels of GIC current duty. With relatively minor modifications to core and clamping structures, it has been found that designs can successfully withstand the additional thermal duty from reasonable amounts of GIC. This functionality has been validated with full-scale GIC tests of single-phase transformers in Siemens Power Laboratories. This means that new power transformer designs can achieve necessary GIC withstand through the use of validated design software.

Recovery Actions

Sparing improvements can be either component-based or achieved via the nearby staging of an entire LPT spare.

In the component case, equipment vulnerability or recovery can be improved by the local warehousing of components vulnerable to physical security threats. Ready access to such items as bushings, radiators or piping segments may reduce restoration times dramatically and (depending on the nature of the threat) can be effective counter-measures. In addition, various accessories or gauges that are externally-mounted may be candidates for local warehousing. Components that are less vulnerable to external physical impact may also be chosen for storage in advance of damage (such as transformer cabling, or control cabinet enclosure and its devices.)

So the vulnerability of an LPT can be reduced via physical security improvements or more robust reliance on rapid response capacity or improved sparing.

POWER TRANSFORMER MODIFICATION for PHYSICAL SECURITY

In the case of common-mode failure threats, it is becoming more prevalent for asset owners to consider designation of specially-designed LPT spares. Such "resiliency spares" can incorporate features which greatly reduce restoration times and therefore provide more functionality from a resiliency perspective. In contrast, the typical system-wide spare approach provides replacement for a damaged power transformer, but may not lead to immediate restoration of service. This is often due to the spare's challenging transportation logistics and extended installation times.

Therefore, as the deterrent to widespread physical damage, CIP-mandated contingency planning may very well identify use of a Rapid Response transformer or reliance on a National LPT Reserve. This has led the author's company to develop Siemens Pretact®—a comprehensive concept which offers solutions and services that help protect transformer assets, prevent operational failures and react in those cases where the worst system events happen.

Resiliency Transformer Features

The features of a rapid response transformer are typically driven by local, case-specific requirements. Ideally, the asset owner will have completed the threat assessment task described above, and thereby have a clear idea of the necessary features which are required. First to be done is the asset owner's identification of particular threat characteristics. Then the asset owner can define his desired functionality of a "resiliency spare". This functionality will require the transformer designer to provide enhanced installation features, such as:

- 1) Ease of Transportation.
 - Pretact® transformers - single-phase units, compact profiles
 - Reduced tank weights, special design features for emergency service life
 - "Lean" design - quick transportation through narrow streets in major cities
 - Components - pre-packaged and pre-staged for rapid deployment
- 2) Advanced Insulating Fluid (if necessary)
 - Mineral oil insulation –can be avoided to eliminate retention pits
 - Ester fluid insulation (synthetic and natural) –reduced fire & spillage hazards
 - Ester fluid insulation (synthetic and natural)–improved thermal performance & reduced footprint
- 3) Ease of Installation
 - Units stored as pre-filled – fluid fill & treatment time eliminated
 - Plug & Play bushing design – unique to industry & aids speed of installation
 - Plug & Play (patent pending) – transport/ install/commission within a few days (depending on storage location /condition of the site and available manpower)
 - Cabling & Cooling – speedy install w/pre-fabricated cable & piping
- 4) Modular architecture and Featured Solutions
 - Can meet almost all regional needs – ideal for strategic transformer reserves
 - Combines owner's approved technologies and latest innovations
 - Multiple Ratings (if necessary) – wide MVA range & voltage selection
 - Switching links for adjustable operational voltages (230/115 kV, 138/69 kV)
 - Overload capabilities – matching particular asset owner contingencies
 - Tertiary windings or low-noise design (if necessary)

Resiliency Transformer Applications

Two “resilient transformer” applications have recently been developed by the author’s company, in cooperation with participating transmission owners. Generally, resiliency units focus on ability for rapid deployment, multiple voltage taps, and the ability to maximize electric capacity while minimizing transportation size and weight. To maximize local transportation and installation options, Siemens conceived its new resilience transformers to be as mobile as possible. A versatile design also means that utilities now need fewer mobile resilience units overall. Special plug-in bushings and connections reduce installation time to a minimum without transformer entry and oil handling.⁽²⁾

Example Threat Scenario > Storm Surge

Siemens is providing Con Edison (the utility powering New York City and neighboring areas) with six mobile resilience transformers. This utility had experienced extensive substation flooding in low-lying areas due to the storm surge from Hurricane Sandy. Con Ed’s threat response was to acquire the ability to replace transformers within days rather than weeks, for both recurring extreme weather events and in case of other major substation damage. These Pretact® mobile transformers are multi-purpose, rated 300/150 MVA, 335x138kV (HV) – 132x68kV (LV) (three phase rating – units are single phase 100MVA/each). Their implementation will enable Con Edison to respond to loss of multiple transformers, whereas normal spares or system redundancy may not be sufficient to allow power restoration.⁽³⁾

The mobile transformers are highly optimized for weight and dimension through numerous design improvements. This reflects not only advanced technology, but also the asset owner’s willingness to accept multiple voltage & power ratings, optimized impedance and the use of environmentally-friendly synthetic ester insulating fluid. This resilience solution will help Con Edison quickly restore power to urban areas affected by future storm surges within a few days, compared to the weeks it may take to transport and install normal available spare units.

As represented in their “installed” position in an urban substation (see Figure 1 below), Pretact® mobile units are pre-filled and stored on dedicated trailers. The use of single-phase transformers and design optimization permits a major reduction in size and weight. The mobiles’ “lean” profiles on trailers allow easy transport through tight urban streets and into cramped urban substations. Flexible plug in cable connections are used to complete bus and phase connections, while pre-filling and use of plug-and-play bushings eliminate the need for long duration assembly of the transformer.

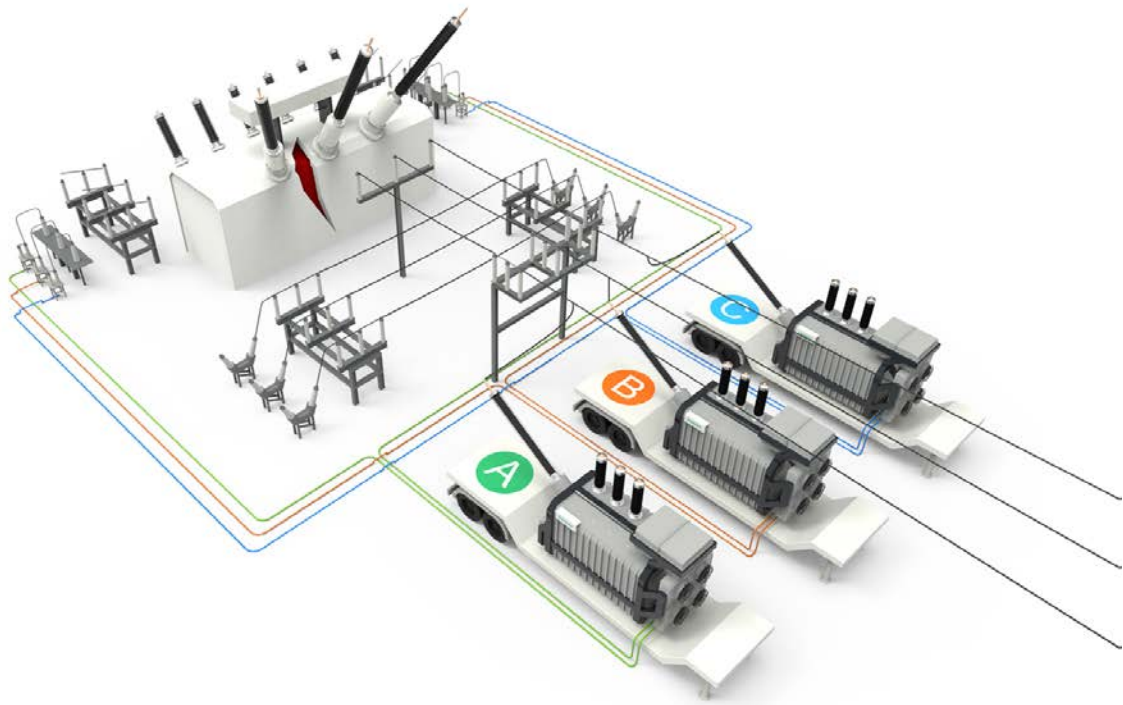


Figure 1. Single-phase Resilience Transformers to Replace Damaged Urban Transformer

“The team from both companies used their extensive knowledge, experience and willingness to depart from the norm to come up with this...unique and innovative design”, said Sanjay Bose, Vice President Central Engineering for Con Edison. ⁽³⁾

SUMMARY

There is increased concern about major weather events or physical attacks to substations and power transformers. The widespread damage caused by major disruptive events may require application of rapid response transformers, since conventional power system redundancies may not be sufficient to restore power. Enhanced physical security using modified power transformers is achievable, but increased interaction is required between asset owner and manufacturer to achieve increased resiliency.

Differing philosophies of physical security may be adopted against the most common threats by various asset owners. As a result, Siemens has developed its new Pretact® Resilience concept with a variety of features that can be applied for a wide variety of asset owner needs. Resilience transformers are as mobile as possible, and use unique design features to reduce transportation and installation time to a minimum.

James McIver, Siemens EM [Physical Security Challenges and Responses for High Voltage Transformers](#)

REFERENCES and AUTHOR

- 1) James Bane, SANS Institute, "An Overview of Threat and Risk Assessment", Posted as part of the Information Security Reading Room. © SANS Institute 2002.
- 2) Tobias Haring & Claudia Hecht, Siemens AG, "Siemens Transformer contributions to Power System Resiliency", Posted as part of the Siemens Resiliency website, March 2016.
- 3) Press Release, Siemens AG, "Siemens to provide Con Edison with mobile resilience transformers", May 3, 2016.

Jim McIver has over 40 years experience in the North American electric power industry. In January 2004, he joined VA Tech – USA as Technology Director, Transformers Business Division. During Siemens' acquisition of VA Tech, he assisted integration of the two groups' R&D staff. He now serves as Technology Director for Siemens Transformers US, assisting with special product applications.

As Nevada Power Staff Engineer, he managed strategic supply partnerships for design, procurement and maintenance of transformers, breakers and switchgear. During his tenure, over 8000 MVA of Elin transformers, shunt reactors and phase shifters were installed in Southern Nevada.

Mr. McIver was GE Senior Application Engineer and specified phase shifters, provided forensic analysis of transformer field failures and developed gas-in-oil diagnostics for sealed-tank, network transformers. Mr. McIver developed component and assembly techniques for GE's first fiber optic temperature sensors and investigated winding mechanical integrity in advanced (gas-insulated) transformers.

Mr. McIver is member of Eta Kappa Nu and IEEE Transformer Committee, and is Professional Engineer in the State of New York. He earned his MSEE from Rensselaer Polytechnic Institute and has authored IEEE and CIGRE papers on power transformers, engineering economics and harmonics.