http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 08 to 09, 2015
Lima – PERU

D2-03_04

P&C Engineer's Response to Cyber-induced Faults

By

Dennis K. Holstein*
OPUS Consulting Group
US

T.W. Cease
Consultant
US

Galen Rasche
EPRI
US

SUMMARY

When asked, protection and control (P&C) engineers describe their response to a cyber-induced fault, they typically answer with "how is the cyber-induced fault different from other normal operational issues addressed in our design of the protection system and operating procedures?" Study committees B5 and D2 commissioned a joint working group (JWG B5-D2.46) to address this question. They concluded, "There is no difference." Regardless of what caused the fault, the protection system is designed to automatically initiate trip actions to safe the primary system or allow it to degrade gracefully so as to allow P&C engineers sufficient time to implement remedial actions. JWG supports this conclusion by examining system dynamic model representations of the fault initiation and automated response. An effective cyber-attack requires practice to refine the attack procedures and timing. When attacks are detected, incident response procedures should require P&C engineers to exercise due diligence by monitoring attack exercises, and where necessary adjust protection relay settings.

Such action requires adequate cybersecurity training for P&C engineers based on three principles. (1) Perception – the ability to sense or detect cyber-initiated fault indicators of relevance for the P&C system's resilience. (2) Comprehension – the P&C engineer's ability to understand the implication of these indicators for the behaviour of the P&C applications. (3) Projection - the P&C engineer's ability to use these indicators to predict or anticipate what variances from predefined protection responses need to be addressed.

Using another system dynamics model, JWG established the relationship between high-priority patching of P&C components to mitigate the software vulnerabilities that an attacker can exploit. This model identifies the critical time delays to implement and deploy critical patches.

KEYWORDS

Cyber-induced faults, cybersecurity, protection and control system, system dynamics modelling

* 628 Island View Drive, Seal Beach, California 90740-5737, USA
Fax: + 01 562 430 1538 e-mail: holsteindk@ocg2u.com

1. Introduction

It is not unusual to find a lack of communication between engineers and field technicians responsible for electric power utility (EPU) substation automation solutions and those responsible for security information technology (IT). This is most evident for protection and control (P&C) operations using operational technology (OT). Constraints imposed by 24/7 operations tend to invert the IT's security paradigm – confidentiality, integrity, availability (CIA) to OT's security paradigm – availability, integrity, confidentiality (AIC).

For example, when P&C engineers are asked to describe their response to a cyber-induced fault, they typically answer with "how is the cyber-induced fault different from other normal operational issues addressed in our design of the protection system and operating procedures?" CIGRE JWG B5-D2 addressed this question and concluded "there is no difference." Regardless of what caused the fault, the protection system is designed to automatically initiate trip actions to save the primary system or cause it to degrade gracefully so as to allow P&C engineers sufficient time to implement remedial actions.

JWG supports this conclusion in their technical brochure #603 published in December 2014[1]. The technical brochure is 121 pages in length including 30 figures and 13 tables. Annex A is a comprehensive list of definitions and acronyms used in the technical brochure. Annex B is a list of 69 references cited in the technical brochure. Following is list of the annexes that expands on the main body of the text.

Annex C: Examples of electrical networks impacted by cyber-induced attack

Annex D: Survey of applicable reports, standards and best practices

Annex E: Safely on-boarding personal devices to P&C networks and components

Annex F: Defending P&C systems against cross-scripting attacks

Annex G: Cryptographic hash functions

Annex H: Preventing stack overflow attacks

Annex I: P&C systems need software assurance to ensure scalable trust at all levels

Annex J: P&C engineers contribute to configuration audits

Annex K: Timely identification of suspected threats

Annex L: CySeMol assessment model

Annex M: Key management life cycle

Annex N: Threat consequences on P&C systems and SIPS

Annex O: Deep dive into practical cybersecurity solutions

Annex P: Extending the U.S. recommendations to strengthen cybersecurity position

---

In summary, the technical brochure offers nine recommendations for practical P&C solutions and ten top take away points to remember. This paper focuses attention on one aspect of the problem – how should P&C engineers respond to a cyber-induced fault.

2. Real world examples of 'normal' operations to evaluate cybersecurity impacts

A report by ENISA [2] on industrial control system (ICS) for computer emergency response capabilities (CERC) or ICS-CERC depicts the capabilities that a computer emergency response team (CERT) needs to develop in order to provide services for the protection of ICS and ICS networks. Although ENISA's report is about ICS, it has a great deal of good ideas for P&C systems.

2.1 Real-time response to a fault

Figure 1 shows a high-level overview of P&C engineer's response to a cyber-induced fault. In real time (about a quarter of a cycle) the protection system receives measurements related to a fault. Based on the protection relay settings the relay changes state which results in a trip command to selected breakers. A complete understanding of relay setting management is vital to responding to cyber-induced faults.

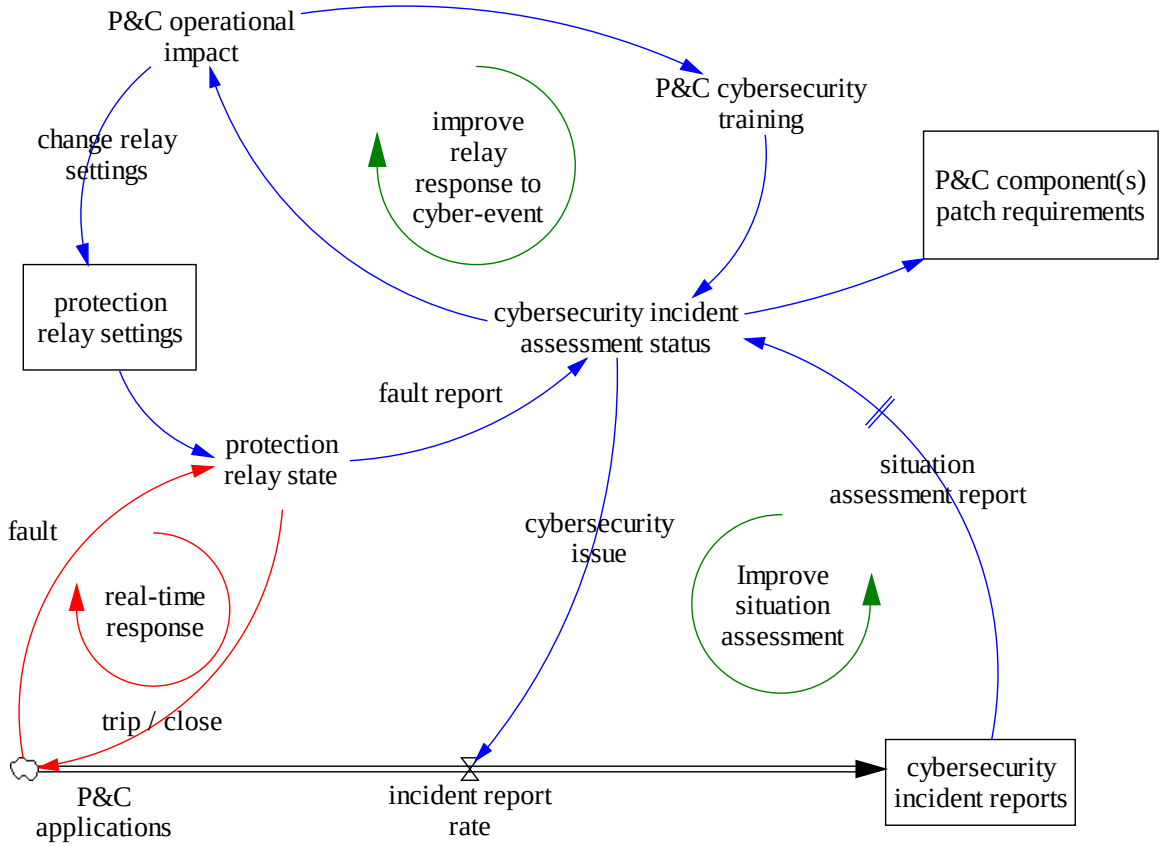

Figure 1 P&C engineer's response to a cyber-induced fault

Figure 1, and later Figure 2, use Vensim's systems dynamic modeling notation [3]. Sterman [4] provides an extensive discussion of modeling business dynamics. Readers are advised to obtain a free version of Vensim PLE for educational and evaluation use to understand the details of the notation.

Note, in red, the real-time response to a fault, any fault, is a trip or close executed by the protection relay. The fault report generated by the protection relay is an input to the off-line post-fault assessment. It is this assessment that may conclude the fault was cyber-induced. If so, the EPU issues an incident report, which may be correlated with other incident reports to generate a situation assessment. As noted by the hashed response (||) a significant time delay occurs between the time when the fault is addressed and when the situation assessment report is available to the EPU cybersecurity team.

Two actions are taken by the EPU's cybersecurity team:

1) P&C component patch requirements are specified and if high priority, patches are deployed to correct the vulnerability exploited by the threat.
2) In the interim, the P&C engineer, who should be part of the cybersecurity team, could change the protection relay settings to better cope with its response to a cyber-event.

As shown in Figure 1, cybersecurity incident assessment requires P&C cybersecurity training. This training combined with their P&C system responsibilities is a prerequisite to determine if the fault was cyber-induced.

An effective cyber-attack requires practice to refine the attack procedures and timing. When attacks are detected, incident response procedures should require P&C engineers to exercise due diligence by monitoring attack exercises, and where necessary adjust protection relay settings. Such action requires adequate cybersecurity training for P&C engineers to improve:

1) Their perception to sense or detect cyber-initiated fault indicators of relevance for the P&C system's resilience,
2) Their comprehension to understand the implication of these indicators for the behaviour of the P&C applications, and
3) Their ability to use these indicators to predict or anticipate what variances from predefined protection responses need to be addressed.

Hernantes, et al, adapted an awareness ladder from the petrochemical industry that provides an excellent framework for cybersecurity training [5]. The reference includes a systems dynamics model expressing the relationship between system weaknesses and leading crisis indicators, and a model linking policies to indicators and system weaknesses.

3. An example use case – high priority patching of P&C components to mitigate software vulnerabilities

Wiik, Gonzalez, Lipson and Shimeall presented a comprehensive paper to the system dynamics society in 2004 titled "Dynamics of vulnerability – modelling the lifecycle of software vulnerabilities [6]." Figure 2 shows some of the dynamics that result in P&C engineers setting a high-priority to patch the vulnerable P&C components. This system dynamics model provides a good point of departure for P&C engineers to justify acceleration of critical patch development and deployment of these patches. The objective is to reduce the number of vulnerable P&C components and increase the number of hardened P&C components.

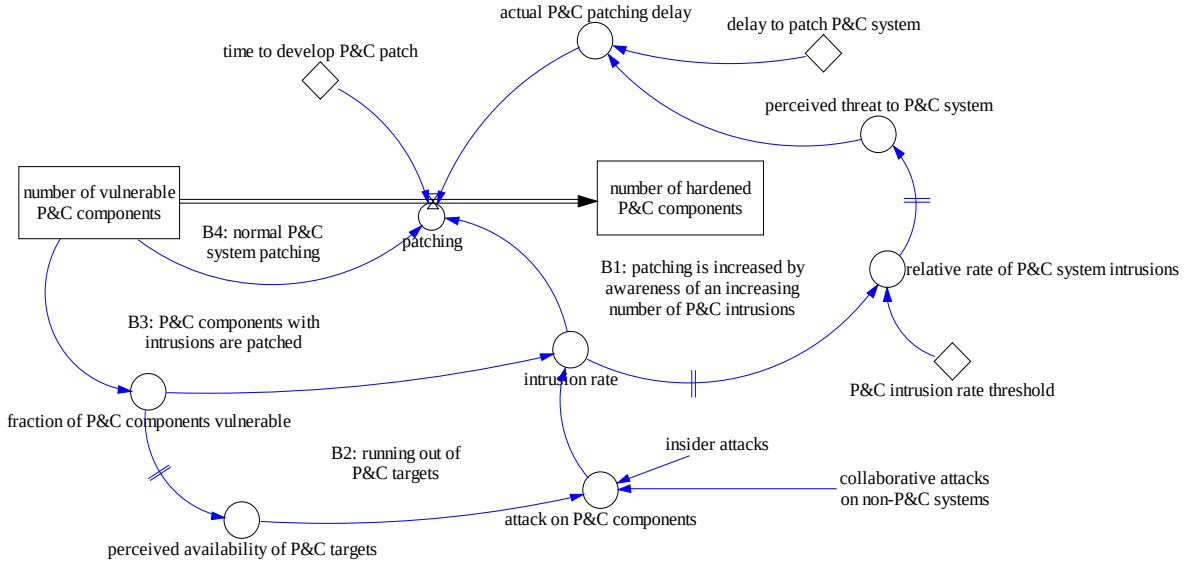

Figure 2 High-priority patching of P&C components

The model implements four system balancing loops. It does not address the potential to introduce additional vulnerabilities when installing patches. To address this issue, the recommendation is to conduct extensive testing in the EPU's quality assurance laboratory.

B1: shows patching is increased by awareness of an increasing number of intrusions. This awareness has a strong influence on the protection engineer's proactive participation in cybersecurity incident assessment discussed previously.

B2: shows that patching reduces the number of P&C targets because installing more and more component patches, the number of targets available will drop. This has an imminent effect on the intrusion rate, but with a delay (indicated by the || on the connectors). It also influences the rate of attack as insiders and their collaborators find fewer targets.

B3: shows that patching vulnerable P&C components also reduces the intrusion rate when compared with the normal P&C system patching labelled B4.

P&C engineers should make every effort to minimize the delays shown in Figure 2.

- The P&C system database (for configuration management) includes an up-to-date list of P&C components that are vulnerable to unwarranted access control and use control. Based on the EPU's risk analysis and potential consequences, flagged vulnerable components are perceived to be high value targets and therefore warrant frequent monitoring.
- Insider (P&C employees and P&C support vendors) attack on P&C components and collaboration attacks on non-P&C components are major factors contributing to the intrusion rate. Automating the processing of access control and use control logs to minimize the time required to determine if the intrusion rate has exceeded a predefined threshold is recommended.
- If the P&C intrusion rate exceeds the threshold, the EPU security policy and organizational directives should require the responsible organization to initiate timely P&C management action to mitigate the perceived threat to the P&C system. In some circles, this is known as centralized command and decentralized execution.

BIBLIOGRAPHY

[1] J. W. G. B5-D2.46, "Application and Management of Cybersecurity Measures for Protection and Control Systems," CIGRE December 2014

[2] A. Dufkova, J. Budd, J. Homola, and M. Marden, "Good practice guide for CERTs in the area of Industrial Control Systems," Technical Report,October 2013.

[3] "The Vensim Simulation Environment," vol. Vensim PLE for Windows, 6.2a-1 ed: Ventanna Systems, Inc - Vensim Product Center http://vensim.com.

[4] J. D. Sterman, *Business Dynamics - System thinking and modeling for a complex world*: McGraw-Hill Higher Education, 2000.

[5] J. Hernantes, A. Lauge, L. Labaka, E. Rich, F. O. Sveen, J. M. Sarriegi, *et al.*, "Collaborative modeling of awareness in Critical Infrastructure Protection," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 2011, pp. 1-10.

[6] J. Wiik, J. J. Gonzalez, H. F. Lipson, and T. J. Shimeall, "Dynamics of Vulnerability--Modeling the Life Cycle of Software Vulnerabilities," in *Proceedings of 22 nd International System Dynamics Conference*, 2004.