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

Dennis K. Holstein*
OPUS Consulting Group
US

T.W. Cease
Consultant
US

Galen Rasche
EPRI
US

Joint Working Group B5-D2.46

This paper describes the work of CIGRE's JWG B5-D2.46 which is published in CIGRE Technical Brochure #603 in December 2014. Described in this paper is a summary of the challenges protection and control engineers and technicians face when required to manage cybersecurity applications and process for their systems, subsystems and components. Because the cyber-threat landscape is so ambiguous they must exercise due diligence to protect their mission critical assets

This work is the effort CIGRE Joint Working Group B5-D2.46

Members

Dennis Holstein, Convenor (US), T.W. Cease, Secretary/Editor (US), Charles Newton (US), Janne Stark (FI), Yoshizumi Serizawa (JP), Shigeki Katayama (JP), Johan Maricq (BE), Andre Suhr (DE), Jorge Lalinde (ES), Jacques Sauve (BR), Hannes Holm (SE), Maik Seewald (DE), Goran Leci (HR), Jean-Marie Boisset (FR), Paulo Pereira (PT)

Corresponding Members

Stephen Thompson, Editor (UK), Rodney Hughes (AU), Tendai Chadyia (AU), Michael Fauchon (CA), Jorge Mendes (PT), Jean-Luc Robichaud (CA), Peter Rietmann (CH), Sanjeev Koul (IN), Ubiratan Alves do Carmo (BR), Joseph Weiss (US), Ralph Mackiewicz (US), Scott Sternfeld (US), Alex Wang (US), Chris Huntley (CA), Juergen Kurrat (DE), Keith Stouffer (US), Ludovic Pietre-Cambacedes (FR), Jens Zerbst (SE), John McDonald (FR), Michael Scott (AU), Ralph Langer (DE), Mike Ahmadi (US), Christophe Poirier (FR)

Cybersecurity management challenge

- **Viewpoint - Protection and Control engineers and technicians**
- **Solve the mysteries of cybersecurity**

Training to recognize cyber-induced faults

Difficulties experienced when interpreting and applying applicable standards and guidelines

Real world operating environment

- **Constraints imposed by 24/7 operations**
- **Compensating mechanisms to protect legacy systems**
- **Resource-constrained intelligent electronic devices**

Management of trust for access and use control

- **Protection and control equipment**
- **Protection and control data**
- **Protection and control communication networks**

Technical Brochure 603 is
121 pages in length including 30 figures and 13 tables

Six major chapters

1. **Scope**
2. **Introduction and framework**
3. **Summary of findings and recommendations**
4. **Cybersecurity threats to P&C systems**
5. **Practical solutions for P&C systems**
6. **Real world examples to evaluate threat impact**

16 technical annexes

- **Extensive list of terms and acronyms**
- **69 references cited for extended background information**
- **Annex C: Examples of networks impacted**
- **Annex D: Research survey**
- **Annex E: Safely onboarding personal devices**
- **Annex F: Defending against cross-scripting attacks**
- **Annex G: Cryptographic hash functions**
- **Annex H: Preventing stack overflow attacks**
- **Annex I: Enabling scalable trust**
- **Annex J: P&C contributions to security configuration audits**
- **Annex K: Timely recognition 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: Recommendations to strengthen cybersecurity protection**

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.

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.

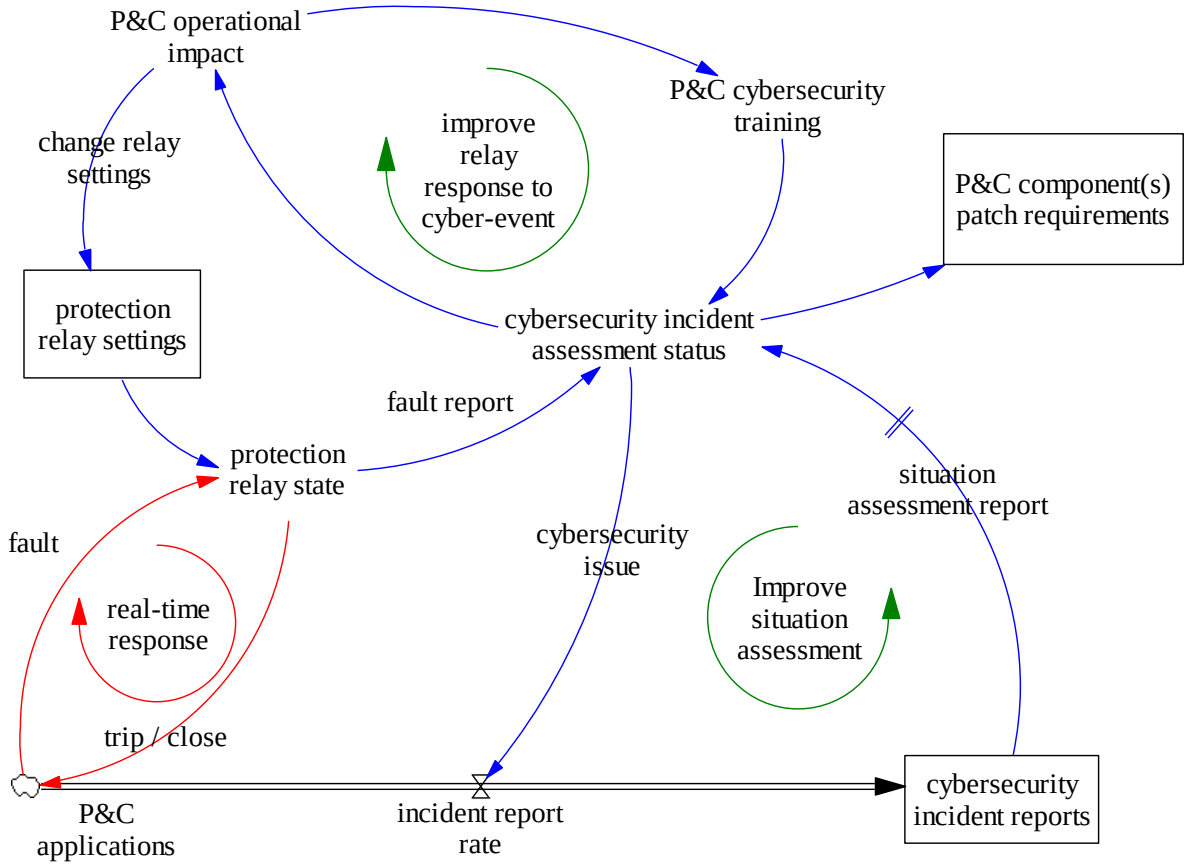

Figure 1

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.

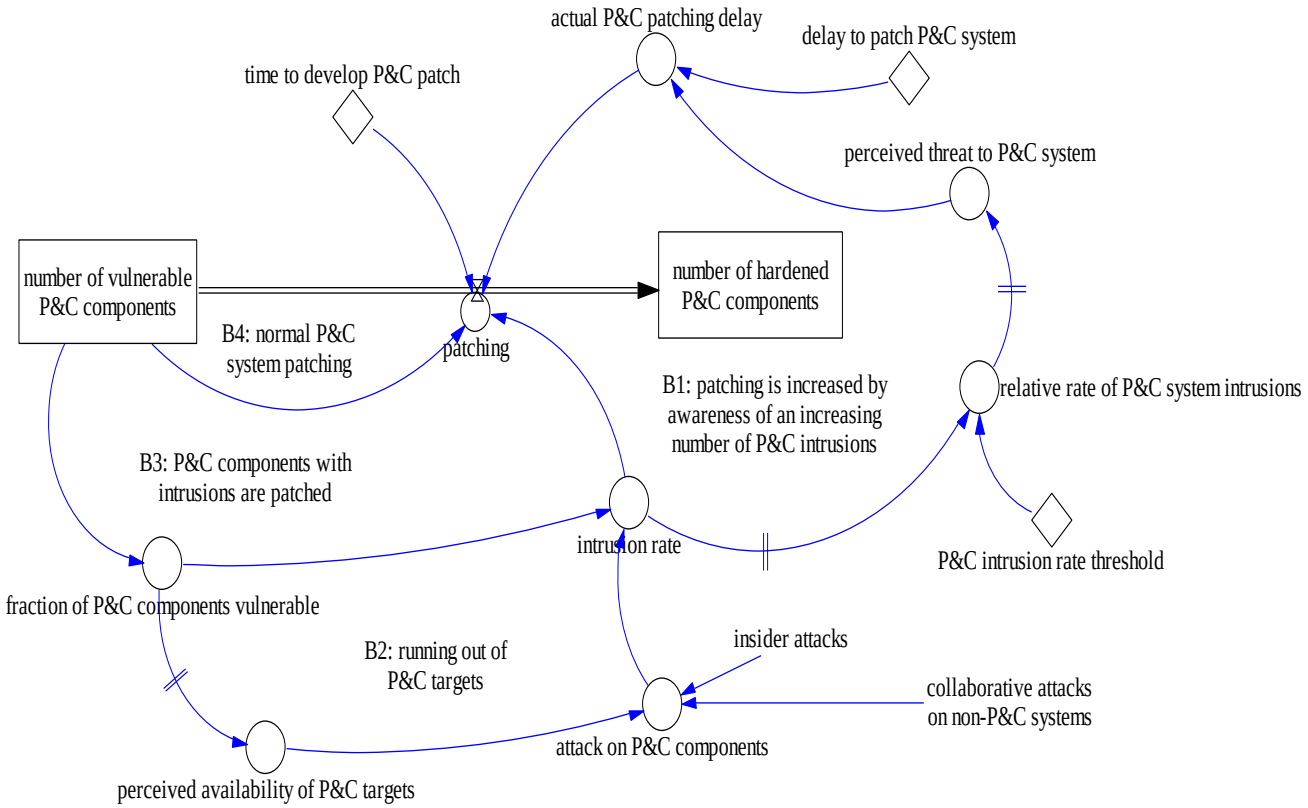

Figure 2

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.

Q3-7. One of the items in this paper is difference of cultures between Information Technology (IT) and Operational Technology (OT). How would you advise to organize OT and reduce the gap between the two groups?

Q3-8. Patch management is becoming crucial in time critical environments. What are the experiences within (or outside) the JWG in deploying patch management. What are the best practices?

Questions?