AUTHOR PROFILE

Rakesh Sharma
Journalist
Freelance Journalist

Follow

Contact

Member since 2006
866 items added with 424,335 views

POST

Cybersecurity: A Systems Approach through STAMP

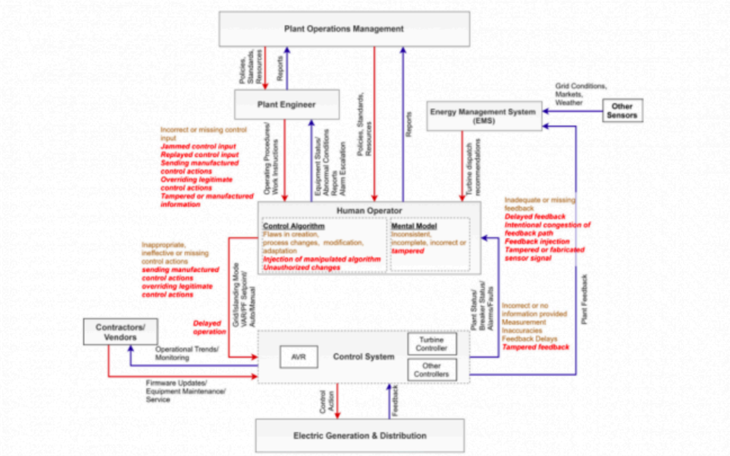

Plant Operations Management
Policies, Standards, Resources
Reports
Plant Engineer
Policies, Standards, Resources
Reports
Grid Conditions, Markets, Weather
Other Sensors
Energy Management System (EMS)
Incorrect or missing control input
Jammed control input
Replayed control input
Sending manufactured control actions
Overriding legitimate control actions
Tampered or manufactured information
Operating Procedures/ Work Instructions
Equipment Status/ Abnormal Conditions Reports Alarm Escalation
Turbine dispatch recommendations
Human Operator
Control Algorithm
Flaws in creation, process changes, modification, adaptation
Injection of manipulated algorithm
Unauthorized changes
Mental Model
Inconsistent, incomplete, incorrect or tampered
Inadequate or missing feedback
Delayed feedback
Intentional congestion of feedback path
Feedback injection
Tampered or fabricated sensor signal
Inappropriate, ineffective or missing control actions
sending manufactured control actions
overriding legitimate control actions
Grid/Islanding Mode VAR/PF Setpoint/ Auto/Manual
Plant Status/ Breaker Status/ Alarms/Faults
Incorrect or no information provided
Measurement inaccuracies
Feedback Delays
Tampered feedback
Plant Feedback
Contractors/ Vendors
Delayed operation
Operational Trends/ Monitoring
AVR
Control System
Turbine Controller
Other Controllers
Firmware Updates/ Equipment Maintenance/ Service
Control Action
Feedback
Electric Generation & Distribution

Figure 10 - Refined Control-Loop for the Operator

image credit: Credit: MIT Study

Share Like (1) Comment (3) Apr 8, 2020 4:02 pm GMT 493 views

In 2015, Russian hackers gained access to Ukranian utility networks and manually switched off power to electrical substations. Hackers were back in 2016, when malware took down a fifth of the country's national capital's grid.

As grids become increasingly automated, both attacks brought home the importance of putting robust cybersecurity practices to protect control systems. They also emphasized the rapidly evolving nature of such attacks. Earlier, cyberattacks were targeted at IT infrastructure. With the rapid advance of algorithms through utility infrastructure, however, operational technology has also become fair game. For example, the 2016 malware disabled a Siemens digital relay, preventing access to circuit breakers.

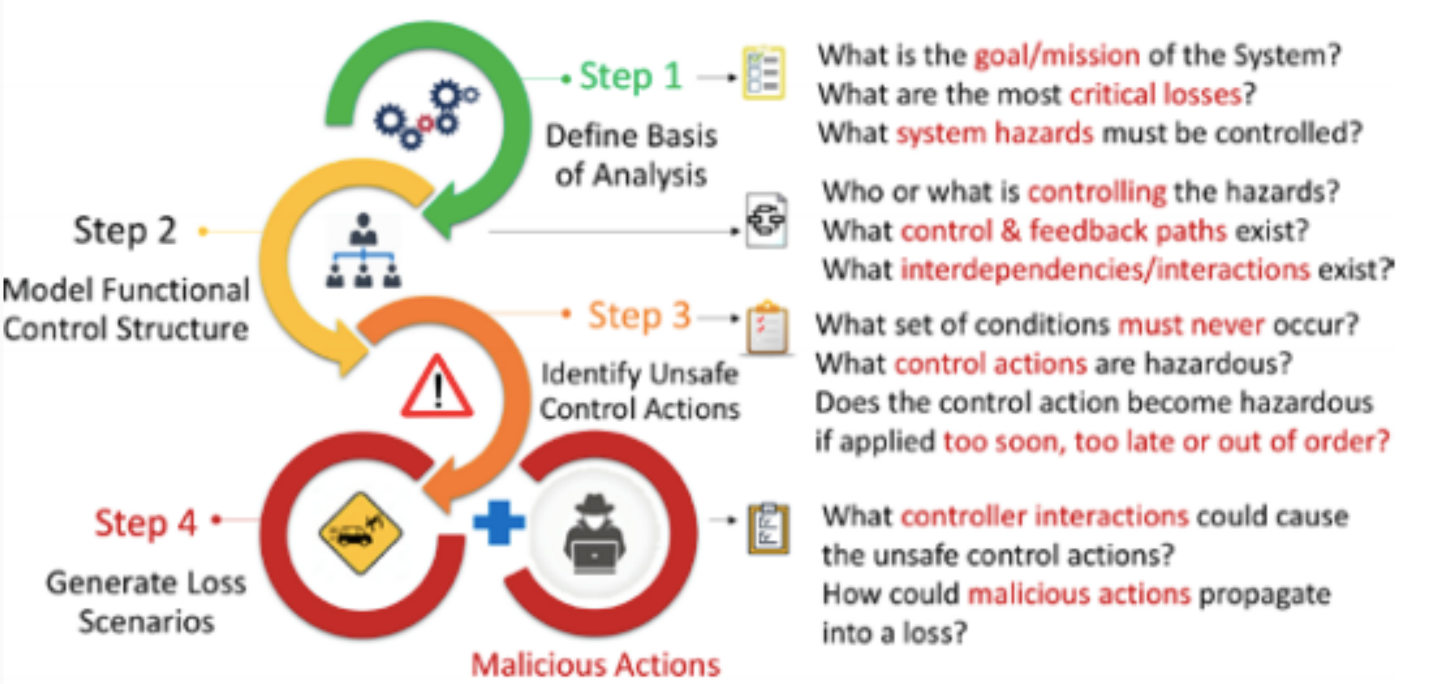
But the view from the grid trenches is not particularly encouraging. A Siemens survey of utilities at the end of last year found that utility checklists and processes for cyber hygiene are aimed at satisfying regulatory mandates for cybersecurity instead of being based off a comprehensive assessment of their internal operations and systems. Cybersecurity investments also tend to prioritize protection of high-value assets, meaning their focus is on ensuring that the most expensive equipment is not damaged or taken offline during an attack. Given the constraints on spending for utilities, that focus makes sense from a financial perspective. But it leaves other assets and infrastructure vulnerable to attacks.

Overarching these problems is an approach based on prevention of cyberattacks rather than containing their impact. That approach is a carryover of traditional information security (IS) practices in which redundancy is introduced into systems to make them immune to attacks. But grid systems are a heterogeneous combination of operational and information technology. In fact, data center servers are below transformers in the equipment hierarchy for utilities. What's more, control elements within the grid system are both automated and manual.

How then should one design a cybersecurity strategy for such systems?

A Systems Approach to Cybersecurity Planning

An MIT study released earlier this year proposes an answer to that question by defining an approach known as Systemic - Theoretic Accident Model and Processes (STAMP). That might sound like a mouthful but it is actually not very different from current approaches in its application. The STAMP process distinguishes itself from other cybersecurity practices by treating control systems in a utility's operations as a single entity and mapping interdependencies between components to find linkages between different pieces. In turn, this helps identify critical components and pieces essential to functioning in case of an attack.


Step 1
Define Basis of Analysis

What is the goal/mission of the System?
What are the most critical losses?
What system hazards must be controlled?

Step 2
Model Functional Control Structure

Who or what is controlling the hazards?
What control & feedback paths exist?
What interdependencies/interactions exist?

Step 3
Identify Unsafe Control Actions

What set of conditions must never occur?
What control actions are hazardous?
Does the control action become hazardous if applied too soon, too late or out of order?

What controller interactions could cause the unsafe control actions?
How could malicious actions propagate into a loss?

Figure 1 - Overview of the Cybersafety Method

The STAMP process begins with defining critical functions necessary for the functioning of a control system. These functions are defined as those losses or hazards that are most critical to the success of the mission or goal of a target system. Thereafter, control loops are refined to simulate various error scenarios.

As an example, consider the diagram above that identifies and evaluates various reasons that might lead to an unsafe AVR command. The erroneous inputs could be generated as a result of human or machine error and cascade down the loop and contribute to a system hazard at the grid level. A subsequent causal analysis reveals contributing factors to the system breakdown. Again, these factors can be a combination of human and machine-generated errors and a post-damage analysis determines the best course of action, whether it is in terms of communication channels or introducing redundancies or checks into the system.

The authors claim that the STAMP approach can result in considerable cost-savings. For example, the introduction of a $6,000 relay helped prevent damage to $11 million worth of transformer equipment based on the results of their study.

Evaluating the STAMP approach

To be sure, the STAMP approach is not novel thinking. Variants of this approach have been used in different industries and are found in disaster recovery literature and planning strategies. But the paper's authors claim that this is the first such instance of its application to the utility industry.

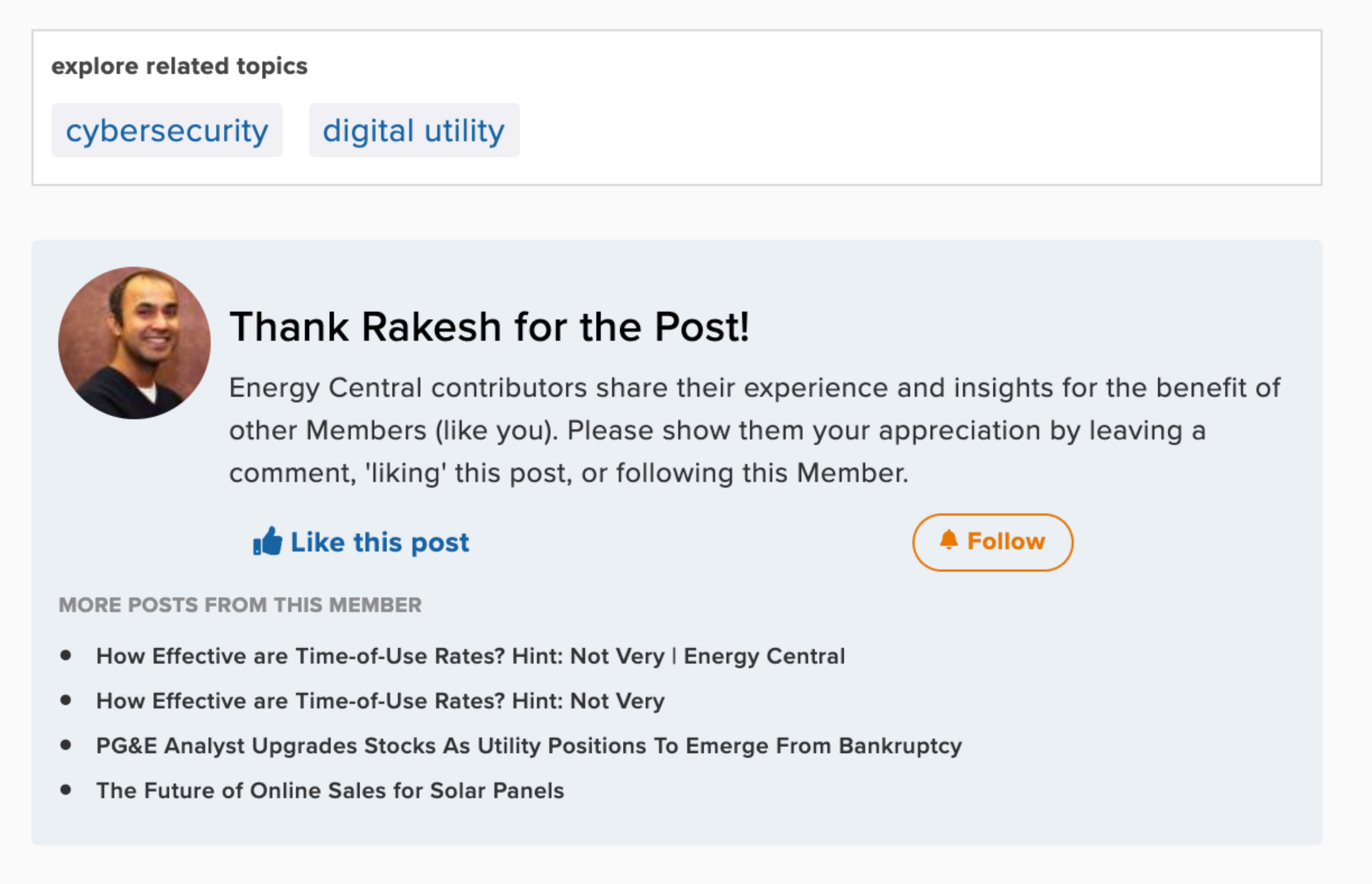
The case study's example is an interesting one. This is primarily because, along with policy and process changes, the approach suggests introduction of redundancy into the system to mitigate the impact of a cyber attack. That redundancy takes the form of the relay mentioned earlier. There are two implications to this.

The first one is on costs. While it may save on expensive breakdown costs, the STAMP process also itself inflates operational costs for utilities. For large utilities, which have expensive asset and infrastructure management budgets, those costs could be considerable.

The second one is on operations. The study does not consider the impact of regulation on the STAMP approach. Various federal and regulatory agencies have started policing cybersecurity practices at utilities. The STAMP approach does not obviate the need for traditional information security practices. It complements and adds to them for effective cyber security practices. But the flip side might be an increase in regulatory overhead.

Does the introduction of new processes and equipment have any effect on compliance measures related to cybersecurity? For example, how might the STAMP approach work with NERC's Critical Infrastructure Protection (CIP) standards? These questions become important when you consider the prospect of a complex, interconnected renewable energy-powered grid in which the number of interconnections between regions multiply.

For all its drawbacks, however, the research takes conversations about cybersecurity in a holistic direction. As utilities increase their spending on cybersecurity practices, they are also looking for efficiencies. Those efficiencies mainly take the form of automation. But Robotic Process Automation (RPA) involves tradeoffs. Even as it reduces costs, RPA increases reliance on machines for control systems. Through its holistic approach, STAMP can help instigate a vital balance between humans and machines during moments of crisis.



explore related topics

cybersecurity digital utility

Thank Rakesh for the Post!

Energy Central contributors share their experience and insights for the benefit of other Members (like you). Please show them your appreciation by leaving a comment, 'liking' this post, or following this Member.

MORE POSTS FROM THIS MEMBER

- How Effective are Time-of-Use Rates? Hint: Not Very | Energy Central
- How Effective are Time-of-Use Rates? Hint: Not Very
- PG&E Analyst Upgrades Stocks As Utility Positions To Emerge From Bankruptcy
- The Future of Online Sales for Solar Panels