Pacific
Northwest
NATIONAL LABORATORY

UOP – Unified Operating Picture

The challenge/need

Critical infrastructure, found in industries such as energy utilities, telecommunications, water and waste control, transportation, and oil and gas refining, depends on industrial control systems to send signals to execute commands. These systems can be especially vulnerable to cyberattacks. So situational awareness is important to operators and defenders.

But expected behavior of industrial control systems varies wildly, making normal operations difficult to characterize and quantify. Standard situational awareness tools are also difficult to use and do not incorporate potentially deviant behavior into operating decisions. This makes operational technology within industrial control systems an attractive target and challenging to defend.

APPROACH

Pacific Northwest National Laboratory has developed a Unified Operating Picture (UOP) that can be used to help make operating decisions in real time through investment in its Proactive Adaptive Cybersecurity for Control (PACiFiC) project.

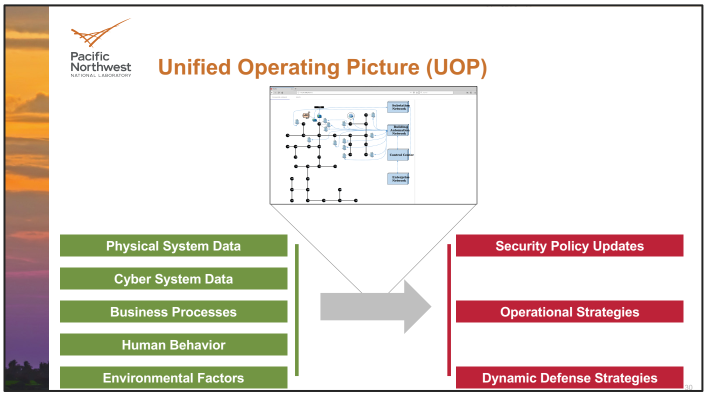
PACiFiC combines adaptive principles, cross-domain information, and classic security best practices to deliver measurably more secure, reliable, robust, and resilient control systems while maintaining system performance. By unifying disparate data and information from across domains, including human, cyber, communications, and process physics, PNNL has defined and established secure design principles for use in all operational technology systems across multiple critical infrastructures and sectors.

HOW IT WORKS

The UOP is an “intelligent dashboard” baseline profile that presents expected behavior of an industrial control system and that can be used to make operational decisions in real time to protect against cyberthreats.

Specifically, the baseline provided by the UOP enables defenders to observe and flag deviations from anticipated system behavior and perform further investigation of indicators from sensors to help ascertain the cause of the event.

The UOP derives operational intelligence by collecting and processing diverse data streams from both the information technology and operational technology environments.



Pacific Northwest NATIONAL LABORATORY

Unified Operating Picture (UOP)

Physical System Data
Cyber System Data
Business Processes
Human Behavior
Environmental Factors

Security Policy Updates
Operational Strategies
Dynamic Defense Strategies

The UOP is a baseline profile of expected behavior of an industrial control system used to make decisions about potential cyberattacks.

UOP uses common information models for storing cyber and electric grid-to-buildings data. The UOP performs multi-domain data mining, cyber-physical alert correlations, and time-place measurement characterization.

The UOP also has the ability to correlate data and generate awareness across domains. It can accurately assess the severity of events based on *all* data.

Examples of data sources include ICS CERT alerts, Automated Detection and Response sensor logs, building automation cyber logs, network Intrusion Detection System (IDS) and switch logs, and cyber and/or physics-based machine learning generated data.

The UOP underpins and integrates all PACiFiC cyber technologies.

BENEFIT

The UOP provides the big picture view of what's happening, so that operators are aware of activity from multiple areas within an enterprise. Correlated technologies help identify whether an event is a potential threat, and the UOP directs operators to take appropriate action.

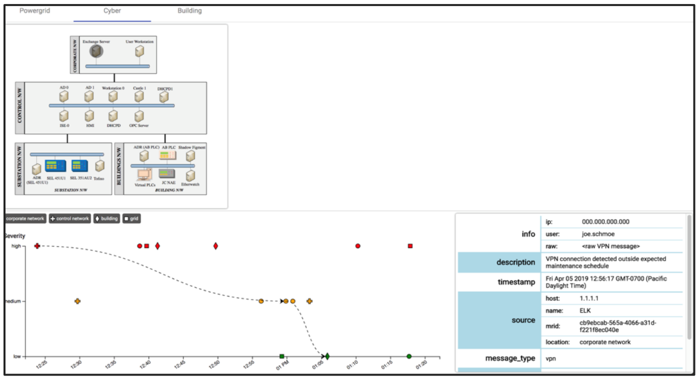
The UOP helps ensure continuity of mission-critical functions in the event of a cyberattack through timely response and recovery.

IMPACT

The UOP accurately captures expected system behavior. Codification allows knowledge continuity from hard-to-acquire expert human analysts, tighter integration with other available data, intelligence sources, and tracking the lifecycle of an adversary.

UOP alerts operators when there is activity that differs from anticipated system behavior such as a potential unauthorized change from a malicious document. It also processes indicators from operational sensors to quickly ascertain the cause and execute appropriate response to a cyber event.

UOP uses existing information to validate unauthorized changes and advises next steps to take based on heightened situational awareness from the rich data sets it incorporates.



info	ip:	000.000.000.000
	user:	joe.schmoe
	raw:	<raw VPN message>
description	VPN connection detected outside expected maintenance schedule	
timestamp	Fri Apr 05 2019 12:56:17 GMT-0700 (Pacific Daylight Time)	
source	host:	1.1.1.1
	name:	ELK
	mrid:	cb9ebcab-565a-4066-a31d-f221f8ec040e
	location:	corporate network
message_type	vpn	

An example alert from the Unified Operating Picture to let operators know something unexpected has happened, indicating a potential cyberattack.

For more information, contact

Siddharth Sridhar
Sr. Power Systems Engineer
Energy & Environment Directorate/Electricity Infrastructure
Pacific Northwest National Laboratory
206.528.3480 | Siddharth.Sridhar@PNNL.Gov

Mark Rice
Electrical Engineer
Energy & Environment Directorate/Electricity Infrastructure
Pacific Northwest National Laboratory
509.375.2435 | Mark.Rice@PNNL.Gov

www.pnnl.gov