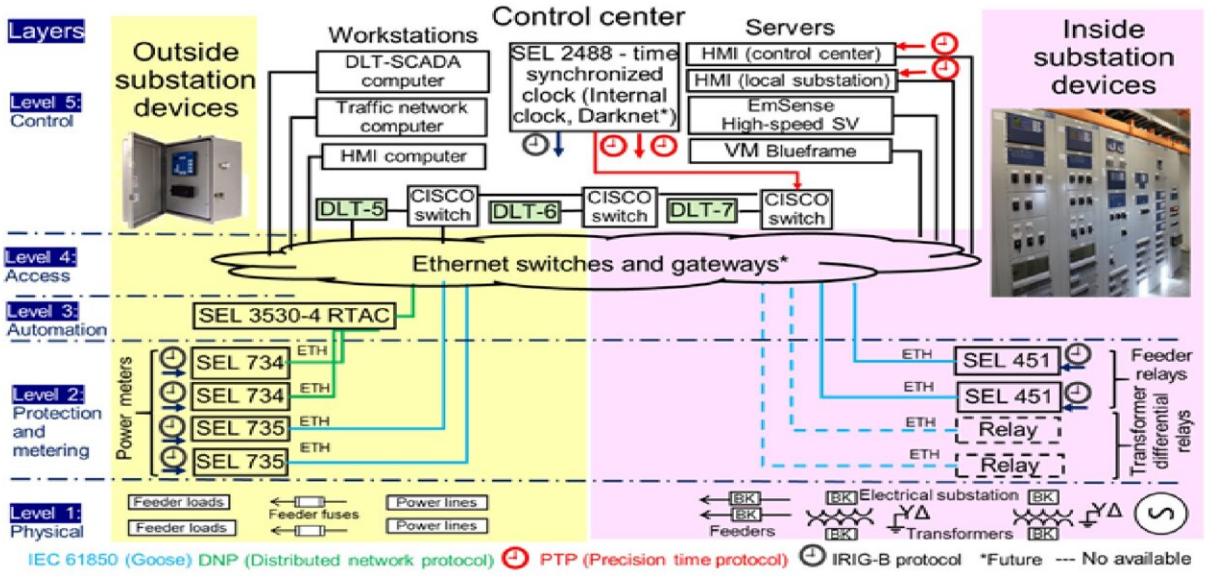
Researchers use blockchain to increase electric grid resiliency

November 23 2022, by S Heather Duncan



Grid Guard substation test bed implementation. Credit: *Oak Ridge National Laboratory* (2022). DOI: 10.2172/1887685

Although blockchain is best known for securing digital currency payments, researchers at the Department of Energy's Oak Ridge National Laboratory are using it to track a different kind of exchange: It's the first time blockchain has ever been used to validate communication among devices on the electric grid.

The project is part of the ORNL-led Darknet initiative to secure the

nation's electricity infrastructure by shifting its communications to increasingly secure methods.

Cyber risks have increased with two-way communication between grid power electronics equipment and new edge devices ranging from solar panels to electric car chargers and intelligent home electronics. By providing a trust framework for communication among electrical devices, an ORNL research team led by Raymond Borges Hink is increasing the resilience of the electric grid.

The team developed a framework to detect unusual activity, including data manipulation, spoofing and illicit changes to device settings. These activities could trigger cascading power outages as breakers are tripped by protection devices.

"This framework gives us a totally new capability to rapidly respond to anomalies," Borges Hink said. "In the long run, we could more quickly identify an unauthorized system change, find its source and provide more trustworthy failure analysis. The goal is to limit the damage caused by a cyberattack or equipment failure."

The approach uses tamper-resistant blockchain to spread configuration and operational data redundantly across multiple servers. The data and equipment settings are constantly verified against a statistical baseline of normal voltage, frequency, breaker status and power quality. Equipment settings are collected at frequent intervals and compared to the last good configuration saved in the blockchain. This allows rapid recognition of when and how settings were changed, whether those changes were authorized, and what caused them.

"Our system helps determine in near real time whether a fault was triggered by a cyberattack or induced by natural events," Borges Hink said. "This is the first implementation of blockchain enabling this kind

of data validation between a substation, a control center and metering infrastructure."

This kind of monitoring requires processing a vast amount of information. The blockchain uses a cryptographic method called hashing, where a mathematical computation is performed on the bulk data to represent it as numbers in the blockchain. This saves energy and reduces the space needed to store data. The blockchain processes thousands of transactions per second for each intelligent grid device, validating the contents.

Researchers demonstrated the framework in a test bed within DOE's Grid Research and Integration Deployment Center, or GRID-C, at ORNL. Built under the leadership of ORNL's Emilio Piesciorovsky, the advanced protection lab uses commercial-grade hardware in a closed electrical loop to mimic the architecture of a real substation.

This provides a low-risk way to simulate cyberattacks or accidental misconfigurations. The team's validation framework can detect both. Researchers are extending the approach to incorporate communications among renewable energy sources and multiple utilities.

More information: Gary Hahn et al, Oak Ridge National Laboratory Pilot Demonstration of an Attestation and Anomaly Detection Framework using Distributed Ledger Technology for the Power Grid Infrastructure, *Oak Ridge National Laboratory* (2022). DOI: 10.2172/1887685

Provided by Oak Ridge National Laboratory