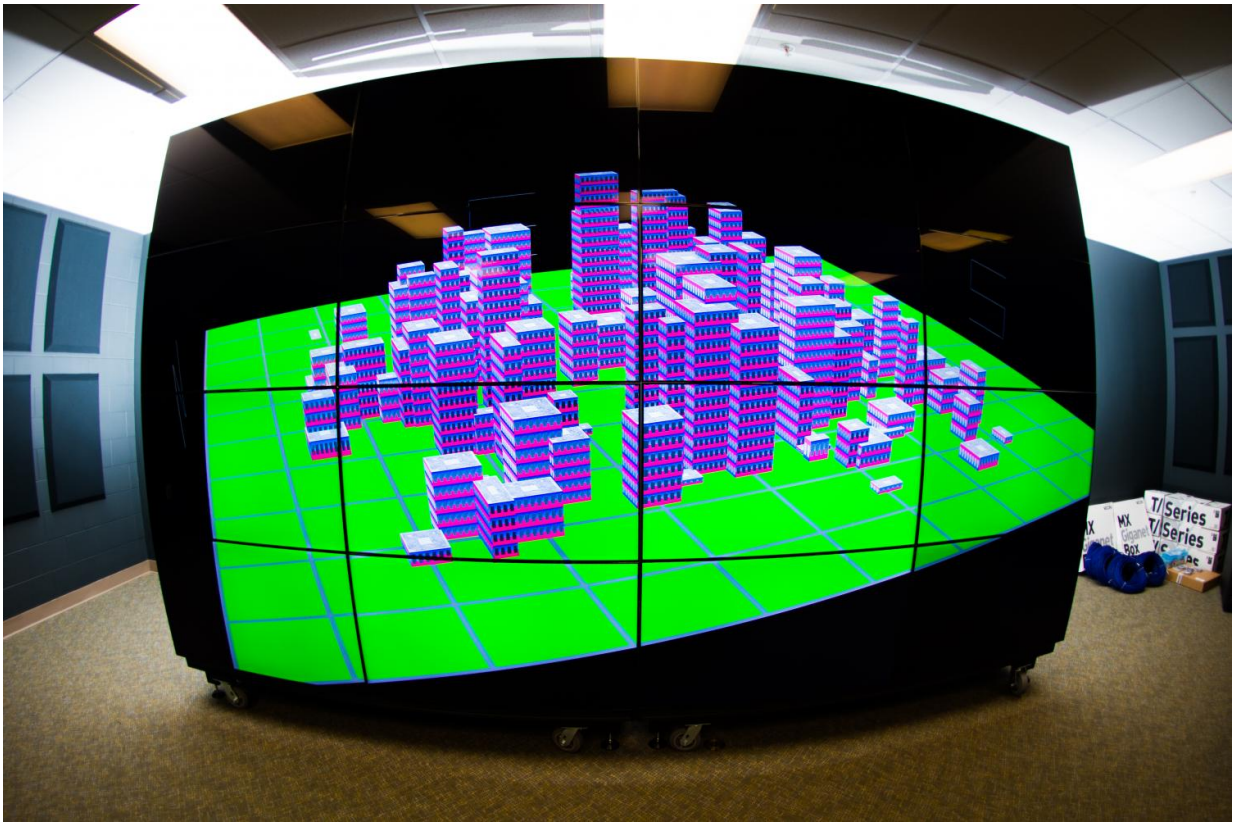
Protecting bulk power systems from hackers

February 10 2017, by Allison Mills



Hackers target specific parts of the control network of power infrastructure and they focus on the mechanisms that control it to cause power outages and blackouts. Credit: Michigan Tech, Sarah Bird

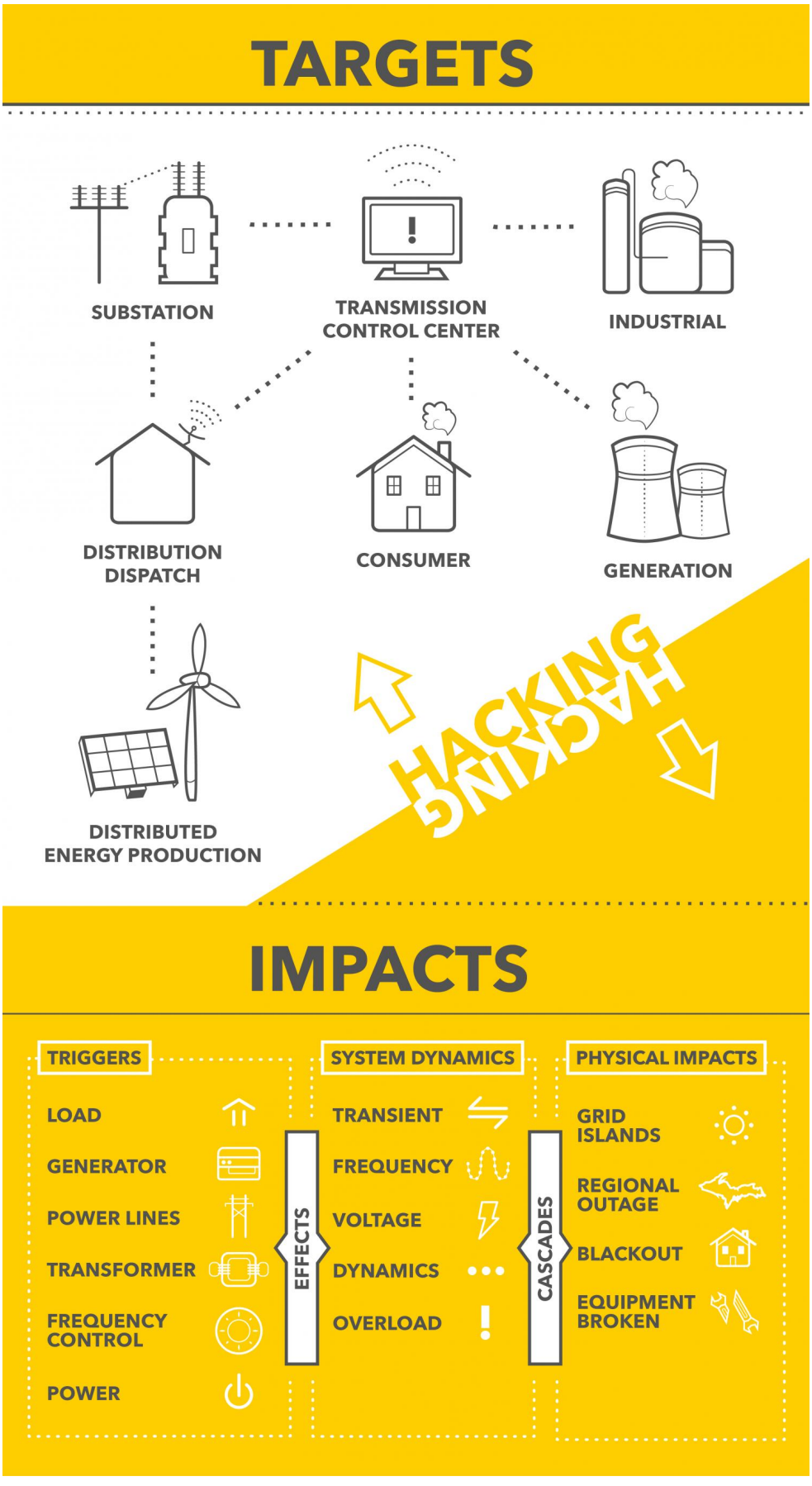
Reliability measures of electrical grid has risen to a new norm as it involves physical security and cybersecurity. Threats to either can trigger instability, leading to blackouts and economic losses.

New research led by scientists from Michigan Technological University delves into so-called "nightmare" scenarios where hackers exploit security weaknesses and execute a disruptive plan of cyberattacks. The journal *IEEE Transactions on Smart Grid* published their work recently. Lead author Chee-Wooi Ten, an associate professor of electrical and computer engineering at Michigan Tech, says the fundamental problem is a gap between physical equipment and intangible software.

Hacked

Advances in smart grid technology—such as smart meters in homes, management systems for distributed energy resources like wind and solar production along with instrumentation systems in power plants, substations or control centers—create both improvements in monitoring and entry points for hackers.

"Ten years ago, cybersecurity simply didn't exist—it wasn't talked about and it wasn't a problem," Ten says, joking that people thought he was crazy for suggesting power grid hacking was possible. "Now with events like in Ukraine last year and malware like Stuxnet, where hackers can plan for a cyberattack that can cause larger power outages, people are starting to grasp the severity of the problem."


TARGETS
SUBSTATION
TRANSMISSION CONTROL CENTER
INDUSTRIAL
DISTRIBUTION DISPATCH
CONSUMER
GENERATION
DISTRIBUTED ENERGY PRODUCTION
HACKING
IMPACTS
TRIGGERS
LOAD
GENERATOR
POWER LINES
TRANSFORMER
FREQUENCY CONTROL
POWER
EFFECTS
SYSTEM DYNAMICS
TRANSIENT
FREQUENCY
VOLTAGE
DYNAMICS
OVERLOAD
CASCADES
PHYSICAL IMPACTS
GRID ISLANDS
REGIONAL OUTAGE
BLACKOUT
EQUIPMENT BROKEN

Specific targets are weak in terms of a power grid's cybersecurity; the impacts hacking have cascading effects through the system leading to equipment failure, power outages, blackouts and islanding where a grid section is cut off from the main grid. Credit: Michigan Tech, Vassilissa Semouchkina

Ten points out that hackers target specific parts of the control network of power infrastructure and they focus on the mechanisms that control it. Automated systems control much of the grid from generation to transmission to use. As Ten puts it, the convenience and cost reduction of automation streamlines the process, but without solid security measures, it also makes the systems vulnerable. The interconnectedness of the grid can also cause cascading impacts leading to blackouts, equipment failure and islanding where regions become cut off and isolated from the main power grid.

Emerging Cybersecurity Threats

Ten and his team draw connections and assess weaknesses using a framework that would constantly assess the bottleneck of a power grid and its interconnection with their neighboring grids. Using quantitative methods to prioritize cybersecurity protection will ensure power grids are operated in a more secure and safer manner. Ten says it's like measuring blood pressure.

"You know your health is at risk because we monitor systolic and diastolic numbers, so perhaps you work out more or eat healthier," Ten says. "The grid needs established metrics for health too, a number to gauge if we are ready for this security challenge."

With a better understanding of the system's weaknesses, it's easier to be strategic and shore up security risks. In the long run, Ten says improving regulations with specifics to match actual infrastructure needs and providing cybersecurity insurance will help.

"Simply because the remote substation networks are constantly commissioned with full compliance doesn't mean they are secure," Ten says. "There is going to be a tremendous impact if we're negligent and fail to keep up with changes in communication infrastructure and emerging security threats."

More information: Chee-Wooi Ten et al. Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems, *IEEE Transactions on Smart Grid* (2017). DOI: 10.1109/TSG.2017.2656068

Provided by Michigan Technological University