Virtual Control Systems for Operator Awareness Training and Cyber Threat Understanding†

Michael J. McDonald & Bryan T. Richardson,
Sandia National Laboratories*
March 29, 2010

† Excerpted from Bryan T. Richardson Motivated Adversaries: What Operators Need to Know, I3P Workshop, Houston, Texas, April 2009

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.
Virtual Control System Environment

- Used to study cyber threat propagation on process control systems
  - Researchers see how cyber threats turn into physical impacts
- Facilitates awareness training
Motivated Adversaries

- Do not play by the rules
  - Will use a full spectrum of methods: cyber, physical, social, etc.

- Have a cause (goal oriented)

- Knowledgeable and smart
  - Understand your system
  - Understand key processes under control
  - Are able to find any back doors your system offers
    - And if you're not watching, they'll keep trying!
  - Know your personnel and your contractors

- Have time on their side
Which Gates Might an Adversary Bypass?

- Firewalls
- DMZ Zones
- Physical Security
- Secure Modems
Some Paths Around the Gates

- Malware insertions
- Worm attacks
- Man-in-the-Middle attacks
- OS & Software exploits
- Pivot & Routing attacks
Possible Mitigations

- Physical/Cyber (integrated) intrusion detection at all levels
- Best practices for network design and segmentation (firewalls)
- Response plan that incorporates cyber attacks
- Physical protection of critical network assets
- Utilize configuration monitoring inherent in control equipment for security
- Organizational response training
Example: Operator Response Training Simulator

Operator's HMI

Simulated Plant

Control Communications

Threat Simulator

Compromised Corporate Workstation

Burner DTUs Turned Up High

Heater Temperature Turned Up High

Supply Pump Turned Off

Heater Explosion

Compromised SCADA Server

Heater Put into Manual Mode

Recirculation Pump Turned Off
In Summary...

- Motivated adversaries have vast amounts of capability at their disposal.
- The possible consequences of a cyber attack are, at worst, catastrophic.
- Operators are a critical element to defending against a cyber attack.
- New technologies are beginning to provide realistic simulators to help
  - Control system designers to understand and protect against the threats
  - Operators to recognize cyber attacks and respond appropriately