Dynamic Software Verification of Industrial Critical Control Systems

Sriharsha Etigowni
4N6 Research Group
Rutgers University
Introduction

• Power grids are old (50 years)

• Smarter power grids
  • more electronics
  • more sensors
  • more cyber parts

• Cyber attacks on power grids
  • cyberwar
  • shutting down facilities
  • targeted attacks
Motivation

• Industrial critical control systems malware’s
  • Blackenergy
  • Stuxnet

• Physical access
  • 450000 high voltage lines
  • thousands of controls

• Safety features required
  • reliability
  • resiliency

• Strong supervision on systems required
Damages in physical world

- Overloading transmissions lines
- Generating excessive power
- Generating insufficient power
- Generating out of sync (voltage angle)
Supervision schemes

• Static (before installing)
  • testing
  • verification and validation

• Dynamic (after installing)
  • monitoring on SCADA/HMI
Required schemes

• Continuous monitoring and supervision
• Live verification and validation
• Close to the system
Advantages

• Reduces intensity of attacks
  • continuously monitoring
  • close to the control system

• Reliable systems
  • reduce after installation attacks

• Reduces infrastructure damage
  • adhere to safety requirements
  • economic benefits
Conclusion

• Verification
  • runtime verification required
  • runtime supervision required
  • always operate in safe conditions

• Close to the plant
  • less damage to infrastructure since safety requirements known
  • less risk of spoofing data