Software Security Assurance of Electrical Grid Systems

C. Warren Axelrod, Ph.D.
Delta Risk LLC

October 24, 2014  Farmingdale State College
IESC 2014

Agenda

• History of electrical grids, communications, and control
• Evolution of threats, expertise, laws
• Mechatronics and software security engineering
• Safety versus security
• Different security and safety perspectives
• Collaboration and communication
• Conclusions
Brief History

• First electrical grid – Thomas Edison, 1882

• Growth of electrical grids – 20th century
  – Physical, electromechanical, electronic controls
  – Dedicated, isolated communications networks

• Appearance of smart grid – 21st century
  – Connections to public networks (Internet)
  – Remote access and control by public, third parties

• Future
  – Artificial intelligence – reduces human intervention
  – Adaptive systems – learn from past experience
Cumulative Threats

• Physical damage, destruction, facility takeover
  – Accidental damage due to human error
  – Intentional – fires, terrorist attacks
  – Acts of nature – hurricanes, earthquakes, floods

• Electromechanical and electronic systems
  – Accidental damage due to human error
  – Electromagnetic pulse – sun spots, intentional attack
  – Fires (South Street Seaport, 1990), floods (Hurricane Sandy, 2012)
  – Intentional – fires, terrorist attacks (9/11)

• Smart grid
  – Accidental damage due to human error
  – Intentional – fires, terrorist attacks
  – Cybersecurity-related – cyber attacks, denial of service
Required Expertise

• Physical facilities
  – Civil, mechanical and electrical engineers
  – Architects, construction workers

• Electromechanical and electronic systems
  – Mechanical, electrical and electronic engineers ("mechatronics" practitioners)
  – Safety engineers

• Smart grid
  – Mechatronics practitioners
  – Software system engineers
  – Safety engineers
  – Cybersecurity professionals
Legal/Regulatory Considerations

• Physical injury, disease, death
  – Electrocution, burns
  – Electromagnetic radiation

• Provision and loss of service
  – Need to provide service for all
  – Bearing of costs of outages

• Liability for faulty systems (safety issues)

• Responsibility for software failures

• Security and privacy
  – Access restrictions for both inside and outside users
  – Data protection – proprietary, personal information
Mechatronics

• Definition
  – Combination of mechanics and electronics
  – “Synergetic integration of mechanical engineering with electronic and intelligent computer control in the design and manufacture of industrial products and processes”

• Scope
  – Mechanical, electronic, control and computer systems

• Limitations
  – Familiar with standalone, isolated systems not subject to external attacks or compromise

• Need for improvement
  – Broaden scope to account for integrated software systems and public network security
Safe and Secure Software Systems

• Definitions
  – Systems engineering: An interdisciplinary engineering management process that evolves and verifies an integrated lifecycle balanced set of systems that satisfy customer needs
  – Safety-critical software: The software must not harm the world
  – Security-critical software: The world must not harm the software

• Scope
  – Safety and security of software-intensive computer systems and communications networks

• Limitations
  – Relatively new fields – lack maturity and experienced practitioners
  – Safety engineering and cybersecurity taught in different departments

• Need for improvement
  – Education and cross training of systems, safety and security engineers
  – Creation and enforcement of generally-accepted standards
Collaboration

• Safety, security and systems engineers come from different educational, training, and job-experience backgrounds
• There are cultural as well as technology differences
• Need education, cross-training and participation of the full set of disciplines throughout the system development lifecycle and in operations and support
• Must examine legacy systems as well as new and prospective systems for security state and capabilities
• Need comprehensive safety and security standards with effective enforcement
Conclusions

- Inadequate recognition that electrical grid environments have changed due to remote access over the Internet
- Little forethought in terms of the future evolution of systems with increasing complexity and interconnectivity
- Inadequate attention to cybersecurity issues
- Lack of universally-accepted cybersecurity policy, guidelines and standards
- Need to incorporate cybersecurity professionals into system development lifecycle for safety-critical systems
- Require senior management support and commitment
- Include attention to security and safety of software-intensive systems in personnel annual reviews, project evaluations, internal and external audits, etc.
Some References

C. Warren Axelrod, PhD
Delta Risk LLC
P.O. Box 234030, Great Neck, New York 11023, USA
waxelrod@delta-risk.net
Telephone: 917-670-1720
About Delta Risk®

• Leader in planning and running cyber exercises
• Delta Risk specializes in:
  – Strategy development
  – Contingency planning, incident response and operations
  – Technical training, exercises, assessments and evaluations
  – Penetration and vulnerability testing
  – Threat awareness and information sharing
  – Advanced cyber education
• For more information, see www.delta-risk.net