Contents

• Who am I?
• Introduction
• Legislative
  • History
  • Cybercrimes & cybersecurity bill – 2017
  • OHSACT
• Standards
• Conclusion
• Questions
Who am I?
• 22 years in industry
• 14 years involved in process networks & security
• ECSA Pr. Eng
Introduction

- Cybercrime reported impact 2015 – R35 billion
- 3rd most active country for cybercrime
- Industrial systems including smart grids at risk
- Aurora – grid specific
- General malware
Legislation - History

ECT Act 2002
Draft CS policy 2010
Establish NCAC / CSIRT 2013
National Integrated ICT Policy Green paper 2014
1st Draft C&C Bill 2015
Revised C&C Bill submitted to Parliament 2017
Legislation – C&C bill

- Chapter 2 – definition of crime:
  - Unauthorised access
  - Interference with data & essential services
  - Failure to comply can result in 2 year sentence

- All NKP’s are automatically included

- Responsibility of owner / operator of critical information infrastructure
  - Apply to have the infrastructure declared critical
  - Comply with directives (at own cost)
  - Audits to be performed every 24 months (Section 58)

- Security to be maintained according to national standards

- SSA – concerns expressed
Legislation – OHSACT

• Controversial

• GMR 3 & 4
  • ICS’s can be fined as part of machine assemblies
  • Securing & safe operation regulations apply

• MHI Regulation 6 (Generally not applicable to Electricity distribution)
  • Risk assessments
  • Audits
  • Mitigation of risk
Standards – SANS62443-2-1
• SATS62443-1-1 also accepted
• Only part of IEC62443 suite
• CSMS
  • Risk analysis
  • Addressing the risks
  • Monitor and improve the CSMS
• Dependant on 2 principles
  • Defence in Depth (DiD) – this includes isolation of functional and logical units
  • Continuous monitoring and improvement.
Standards – SANS62443-2-1
Standards – SATR62443-3-1:2016

• Implementation technologies
  • Authentication & authorization – includes password management
  • Filtering / blocking / access control – does not include physical access control, but includes firewalls
  • Encryption & data validation – includes VPN’s
  • Management, audit, measurement, monitoring & detection – includes antivirus, IDS and automated software management
  • IACS software – covers the different operating systems
  • Physical security – access control and personnel security
Standards – SATR62443-3-1:2016

• Industry specific guidelines should be used
  • NERC CIP, NIST, ENISA
Conclusion

• ICS systems at risk
• Legislative impact
• Be proactive
Questions?