

# Industrial Cybersecurity for Electrical Systems

M. Rossouw – Proconics

# Contents

Introduction	01	
	02	Basic SANS requirements
SANS for electrical systems	03	
	04	Incidents
What to do?	05	
	06	Questions

# Introduction

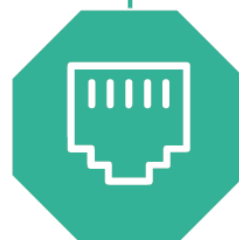
Cybercrime reported impact 2015 – R35billion



On average every industrial system impacted 3 times/year (Kaspersky 2017)



Each connection port a potential entry point



Legislation (CIP bill, King IV)



3<sup>rd</sup> most active country for cybercrime



Some installations experience thousands of attempts / day



South Africa have adopted parts of IEC62443 as SANS62443



# SANS62443 process

Methodology not prescribed, but process is



Zone / Conduit definition



High level assessment:

- GAP analysis & SAL(T) determination
- Zone prioritisation
- Segmentation

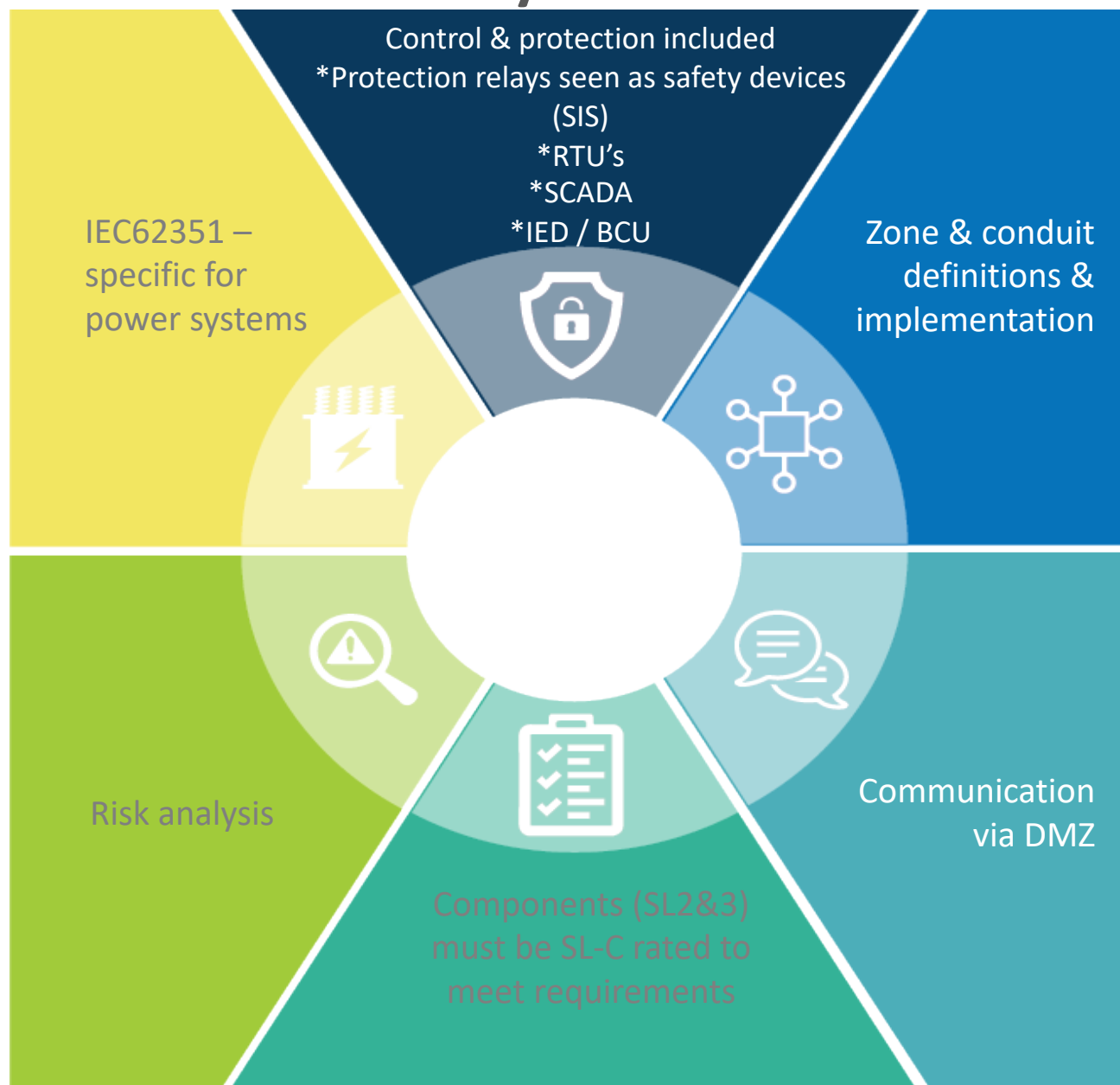


Detail assessment

- System prioritisation
- Base protection according to SL/SAL(T) requirements
- Specific vulnerability prioritisation



# SANS62443 – Electrical Systems?



# Is there a danger?



Aurora demonstration (2007) – specific protection required



Black energy Ukraine (2015)



US grid incidents 2016 –



2019 (DDoS) 10 hour interruption



Local Hacks/Incidents

# What can be done?

Base protection measures  
(based on risk analysis)



Cyber Security Management System (CSMS)

Ensure vendors / OEM's /Contractors can meet SANS62443-2-4 requirements

Prevention is difficult, but early detection, response & recovery critical

Forensic custody chain for repeat incidents analysis

Advanced detection (ML/AI) depend on good baseline

# Conclusion



Energy systems at high risk



Multiple serious impacts



Management requires structured & continuous approach



Base protection just a starting point, but critical



Detection, Response & Recovery





# Questions?

