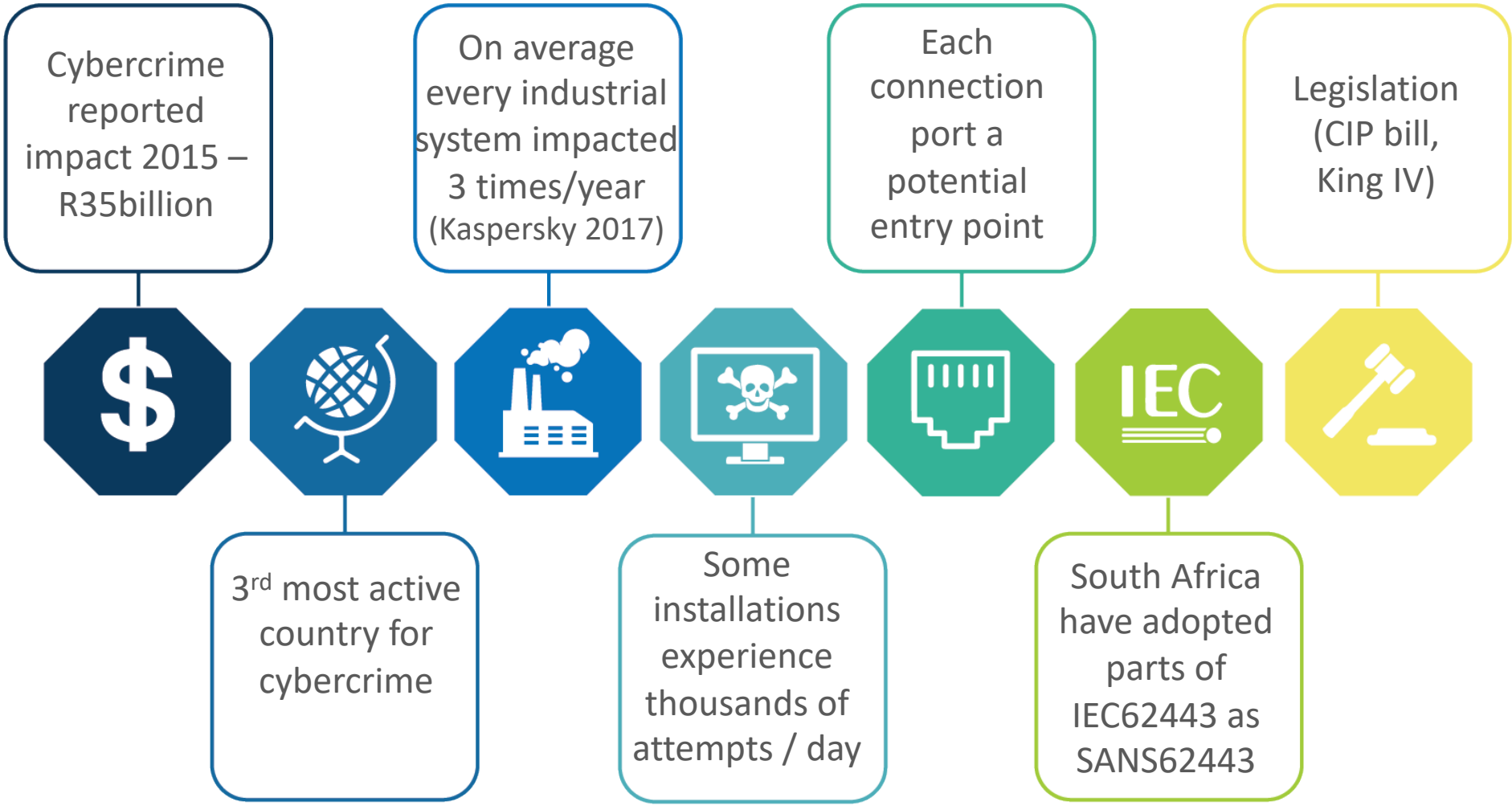
Industrial Cybersecurity for Electrical Systems

M. Rossouw – Proconics

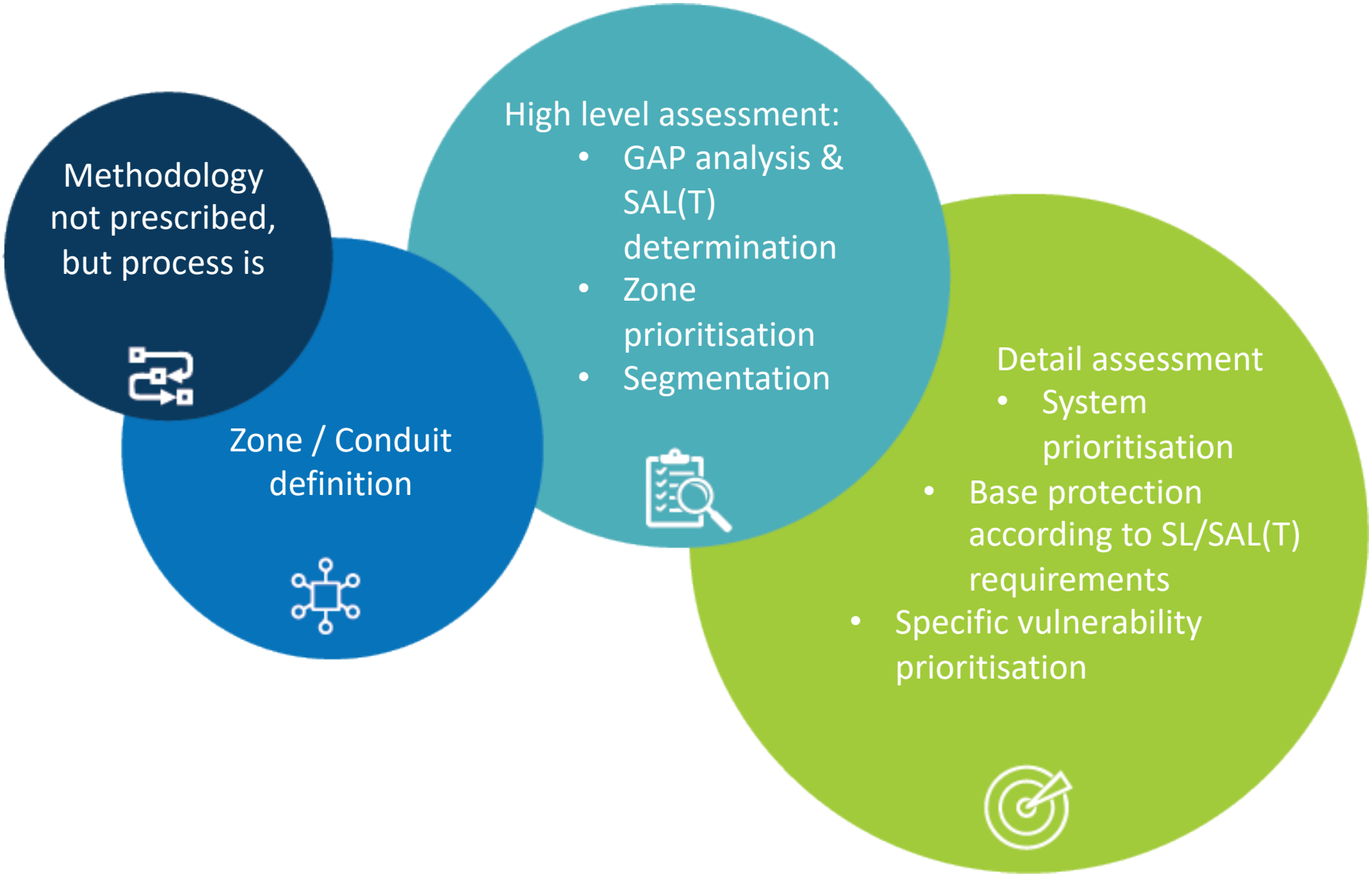
Contents


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

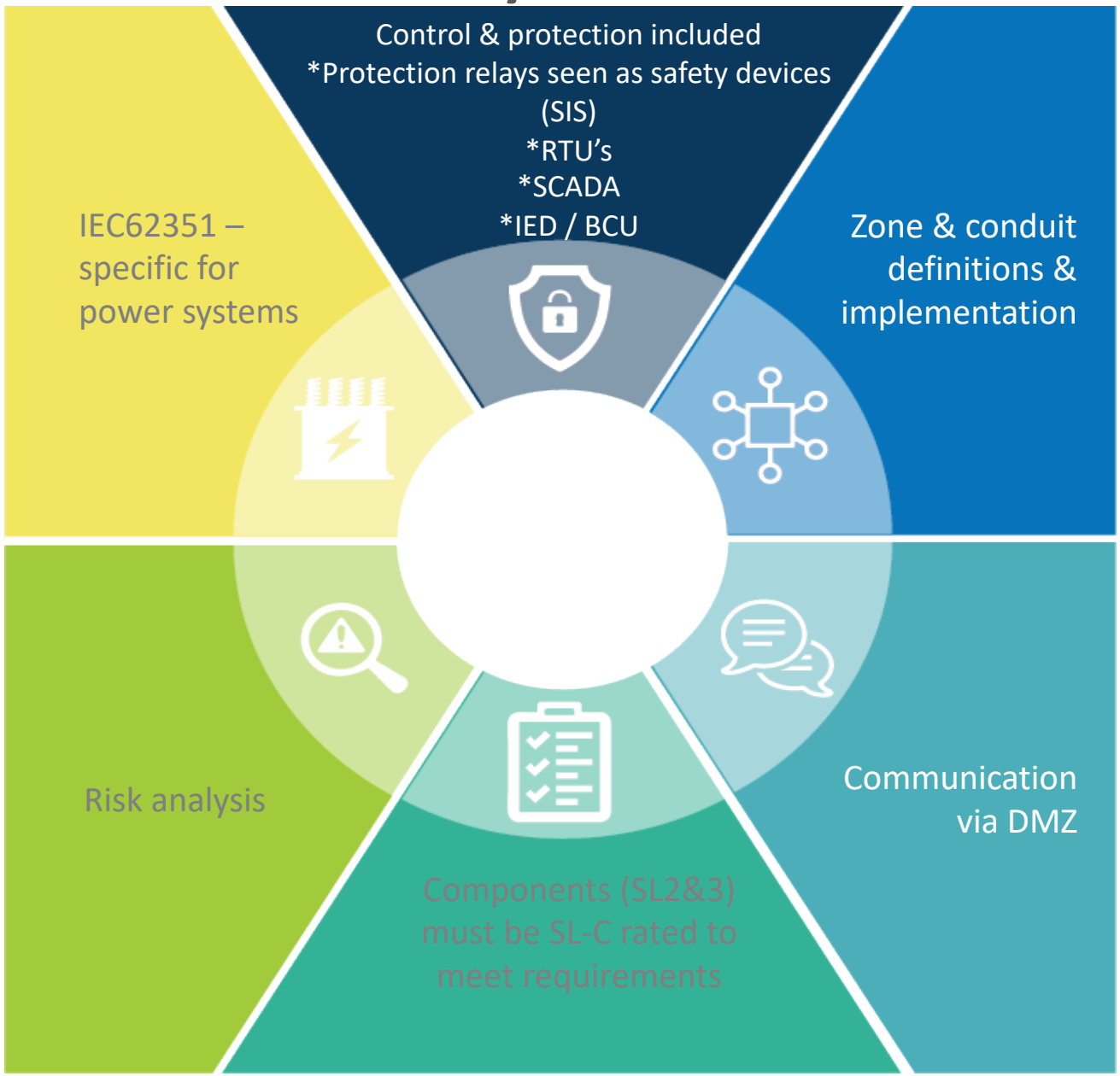
Introduction



SANS62443 process



SANS62443 – Electrical Systems?



Is there a danger?

Aurora demonstration (2007) – specific protection required

Black energy Ukraine (2015)

US grid incidents2016 –

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?