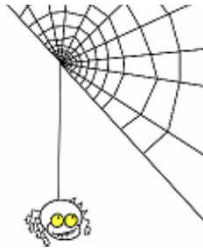
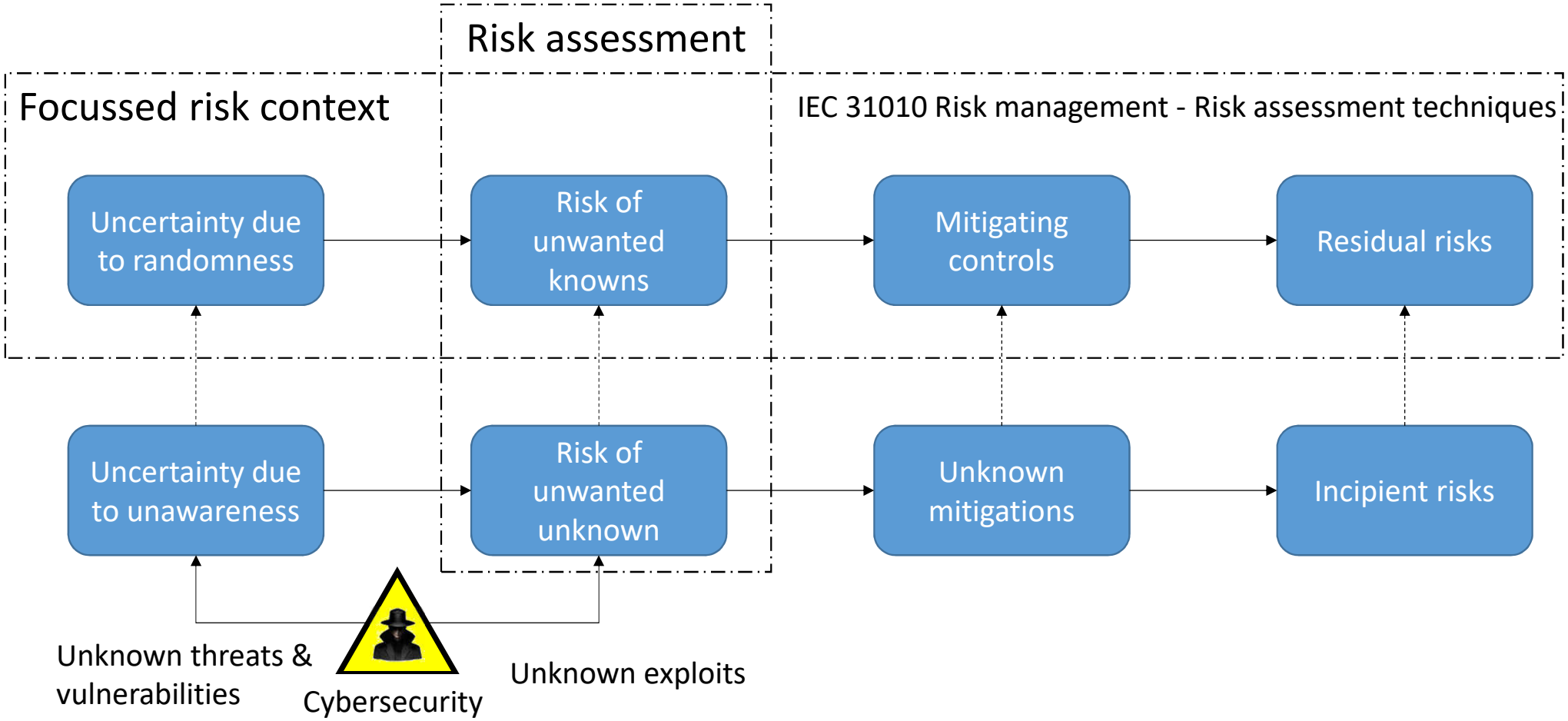


Understanding risk in an entangled world

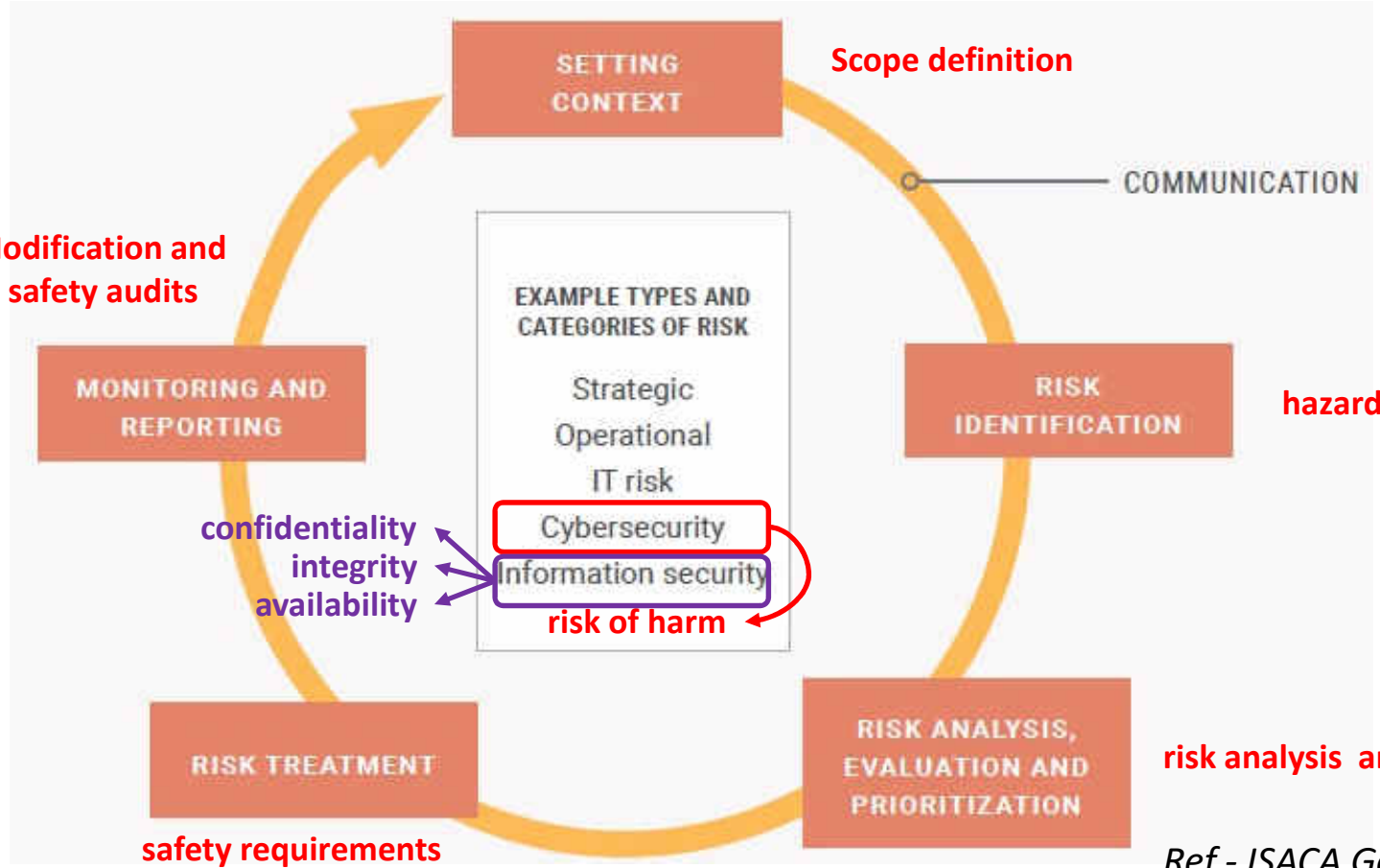
Bruce Hunter

Keynote presentation at 2018 Australian System Safety Conference

Known knowns and the rest…



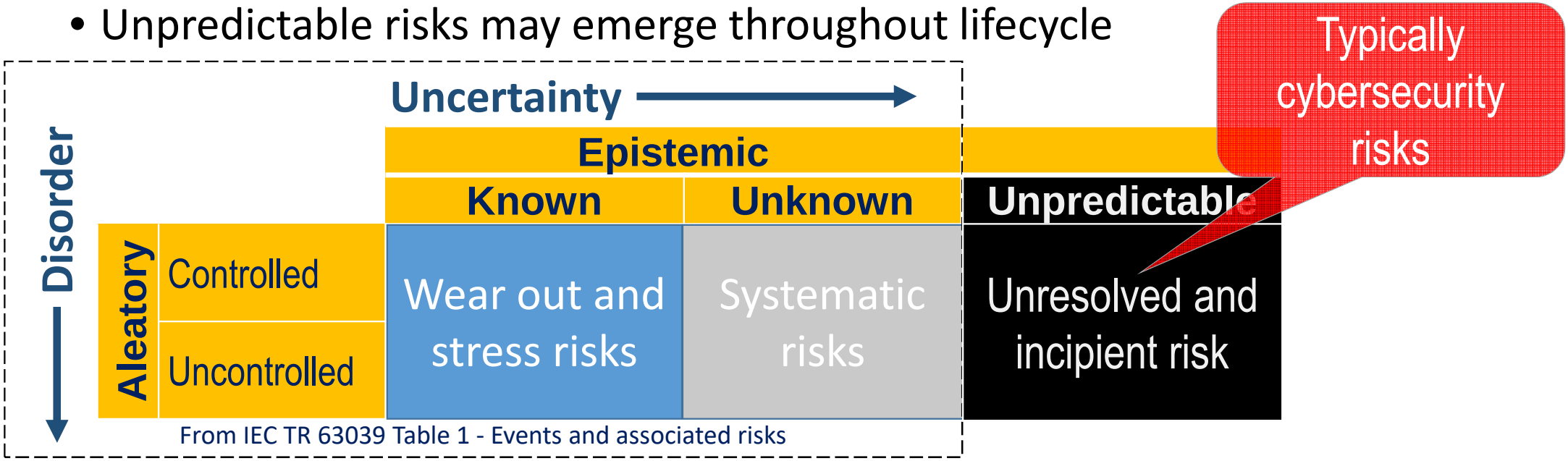
Introduction – IT view of risk types and cycle



Ref - ISACA Getting started with risk management

System failure and entangled risk

- Entangled (connected and persistent) risk context wider that conventional safety risk
- Unpredictable risks may emerge throughout lifecycle



IEC 63039/TR/Ed1: Probablistic risk analysis of technological systems – Estimation of final event rate at a given initial state

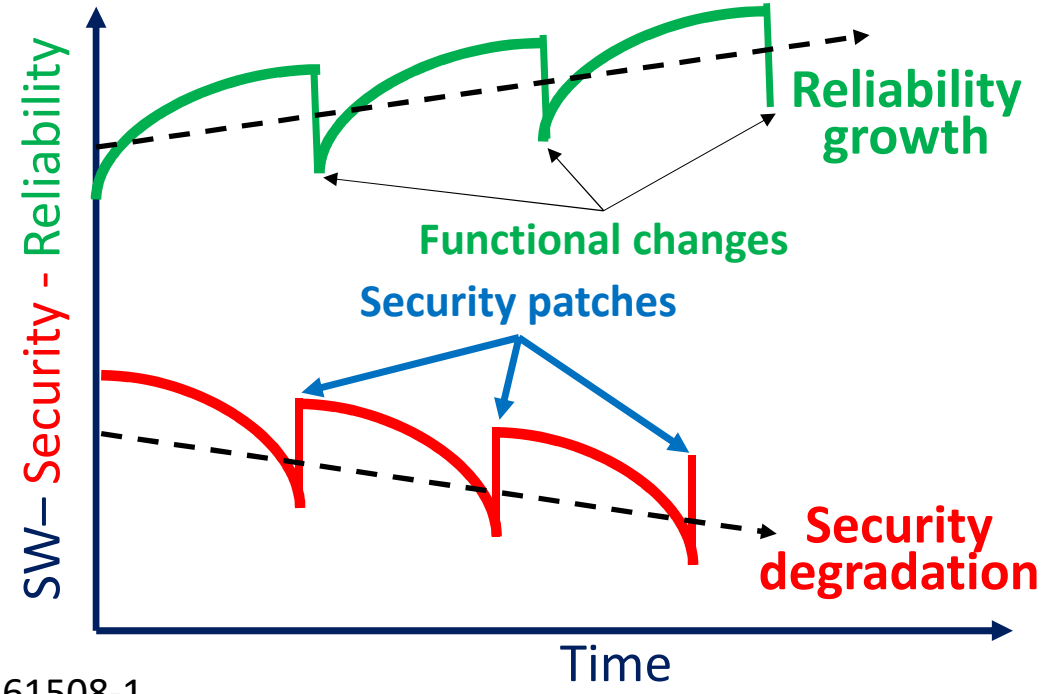
Safety and the air-gap illusion

- Traditional safety systems have relied on physical “air-gapped” architectures for security[1]
- ICS security incidents show the fallacy of physical isolation or simple perimeters alone[2]
  - “Security by obscurity” became “vulnerability by gullibility”
  - Vulnerable in bypasses by people
  - Vulnerability of hidden architectures/dependencies
  - Exploitation of core technology vulnerabilities
- Technology evolves on the premise of connectivity; people evolve to overcome barriers to connection

1-NIST, ISACA, ICS-CERT 2-The wall is the wall – why fortresses fail

The safety/security divergence

- Failure rate/integrity prediction
  - May be calculated from component or system reliability (wear-out) [1]
  - May be claimed if rigour requirements are met [2]
- Exploitation rate dependant on:
  - Evolving threat actor capability and value of target
  - Evolving vulnerabilities and exposures [3]
  - Minimised by applying security requirements [3]



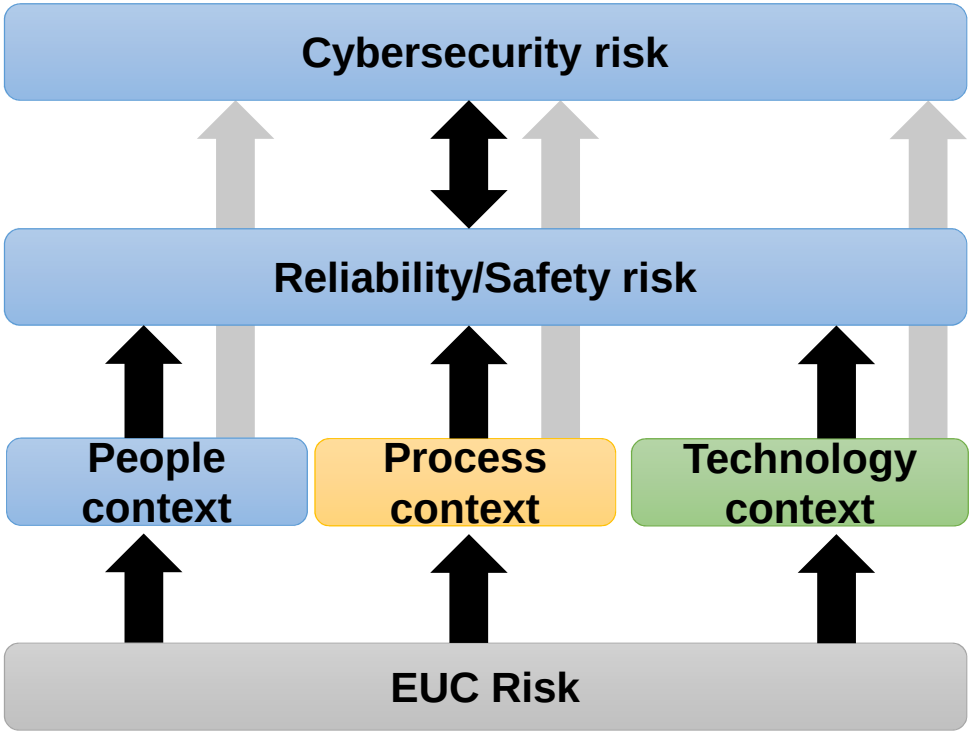
[1] IEC 61508-1
[2] IEC 61508-3, IEC TR 61508-3-1
[3]] IEC TR 62443-3-1 IEC 62443-3-3

Oh what a tangled web we weave…

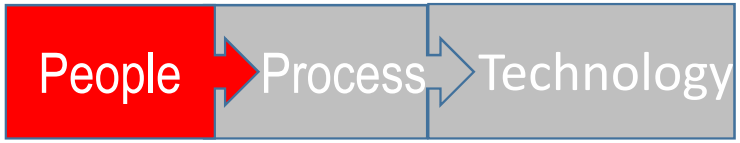
- 2017-2018 infrastructure cybersecurity events
  - July 2017 Industroyer, Crashoverride
    - (ICS-ALERT-17-206-01) – targeting energy sector
  - 2017 ransomware WannaCry(pt)(ICS-ALERT-17-102-01),
  - 2017 Petya/Not-petya (ICS-ALERT-17-181-01) – target Health sector
  - 2017 Intel CPU firmware vulnerability (CVE-2017-5721,572)
  - December 2017 – TRITON/Hatman attack on SIS ESD (MAR-17-352-01, Triconex SEVD-2017-347-01)
  - January 2018 – Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5715,53) – vulnerabilities in x86 CPU chips - (ICS-ALERT-18-011-01)
- Future Black Swans and outliers
  - AI, IOT, etc. etc.
  - Today's "improbables" may become tomorrows realities

Expanded risk coverage needed

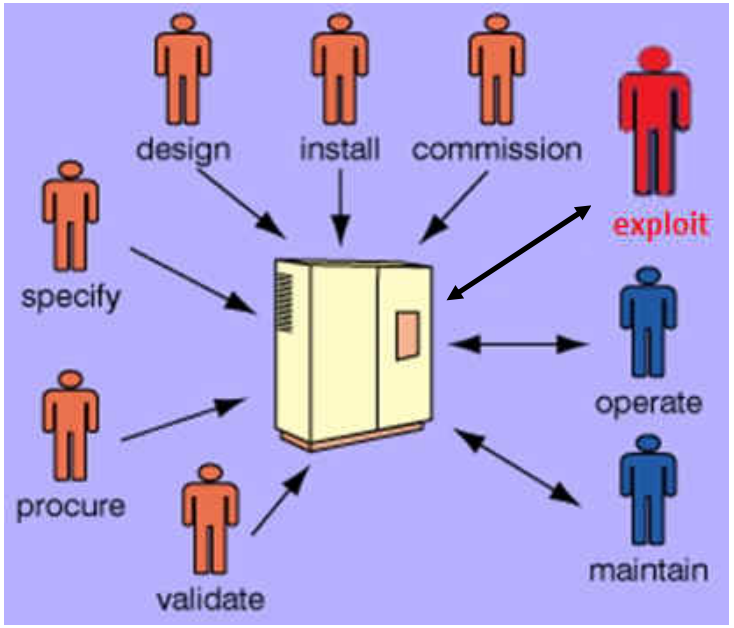
- Equipment failures not enough
- Broaden to ALL influences
  - People
  - Process
  - Technology
- Broaden to ALL risks
  - Reliability/Safety
  - Cybersecurity
  - Manipulation (people & technology)
- Measuring risk completeness?



Human connected security risk



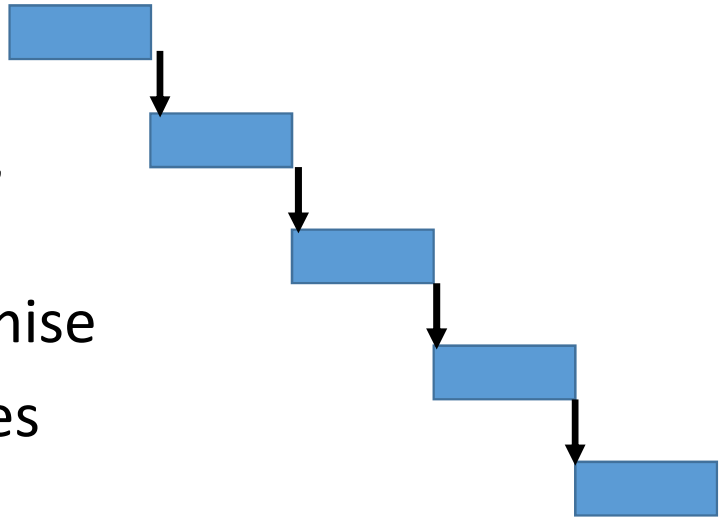
- Humans introduce risk over lifecycle
  - Introduce vulnerabilities accidentally or intentionally
  - Exploit vulnerabilities
- Internal/Insider risks (designers, integrators, testers, operators, maintainers)
  - Fallibility – human dependability - competence -
  - Gullibility – human susceptibility
  - Irresponsibility – human defiance or malice
- External risks (Nation states, cybercriminals etc.)
  - Ransomware, DDOS
  - Malicious control, exfiltration
- Can be driven by Cognitive Bias & Risk Heuristics*
  - Risk of desensitisation in use (Ip, Greg "Foolproof…")
  - Behavioural manipulation



* Perceptions of risk

Process connected risk

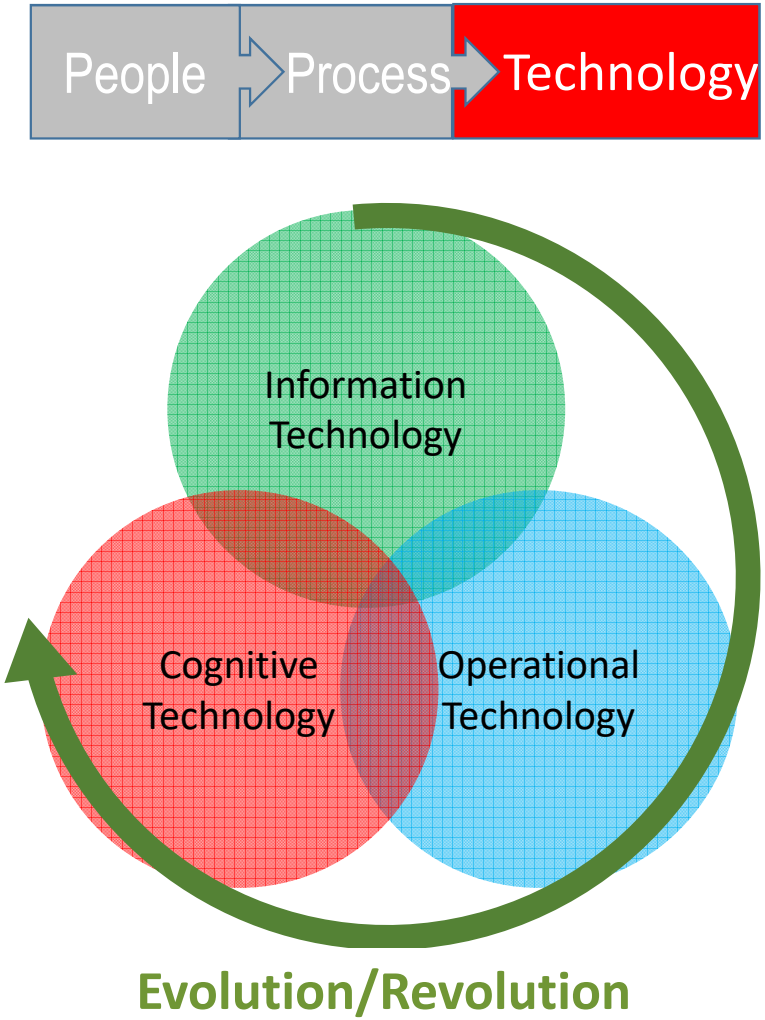
- Risk of configuration tool compromise*
- Risk of development tool infiltration*
- Risk of development and release process errors, including regression*
- Risk of deployment process errors and compromise
- Influence of associated time-to-market processes
  - (e.g. DEVOPS)
- Risk of risk process itself



*Addressed in IEC 61508-3 development requirements

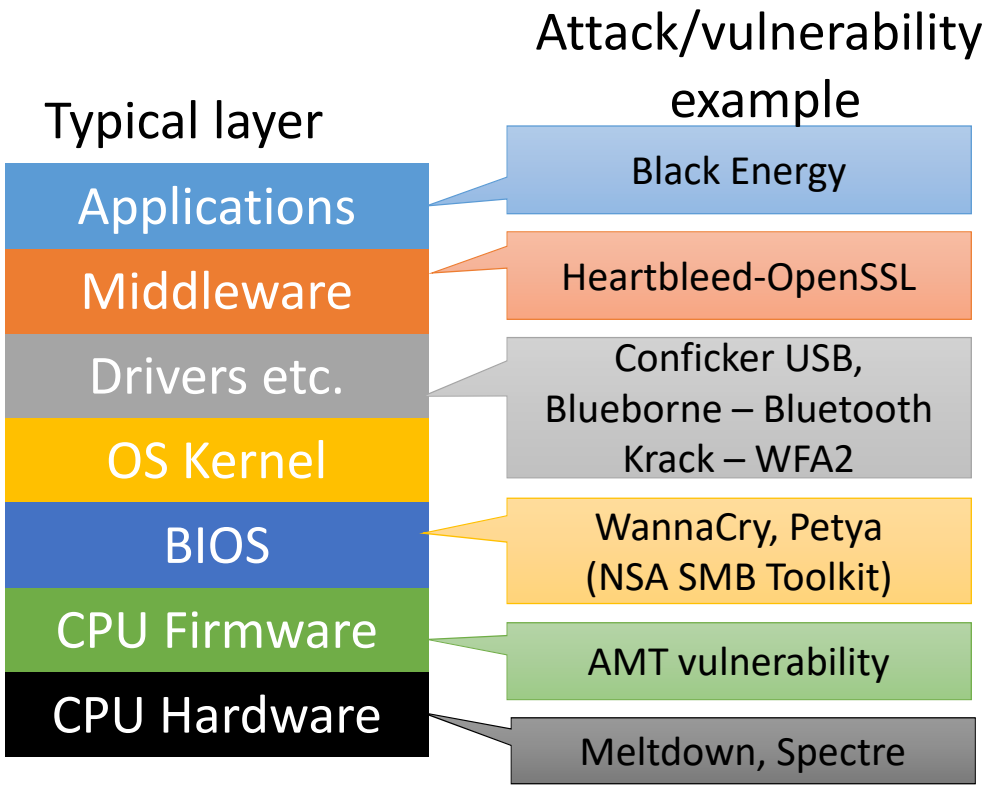
Technology risk context

- Technology emergence/convergence
  - Information Technology (IT)
  - Operational Technology (OT)
  - Cognitive Technology (CT)
- ICS Technology context cybersecurity risks
  - IT technology and COTS risk inheritance
  - Business/Public System Integration
  - Historically poor ICS security stance
  - Difficulty in updates- patches – penetration testing



Technology layer attacks

- Security threat agents look for new vectors
- Protection difficulty increases with layer depth (e.g. Meltdown and Spectre)
- Ingrained vulnerability zero-days (e.g. ix86 vulnerability from 1995)

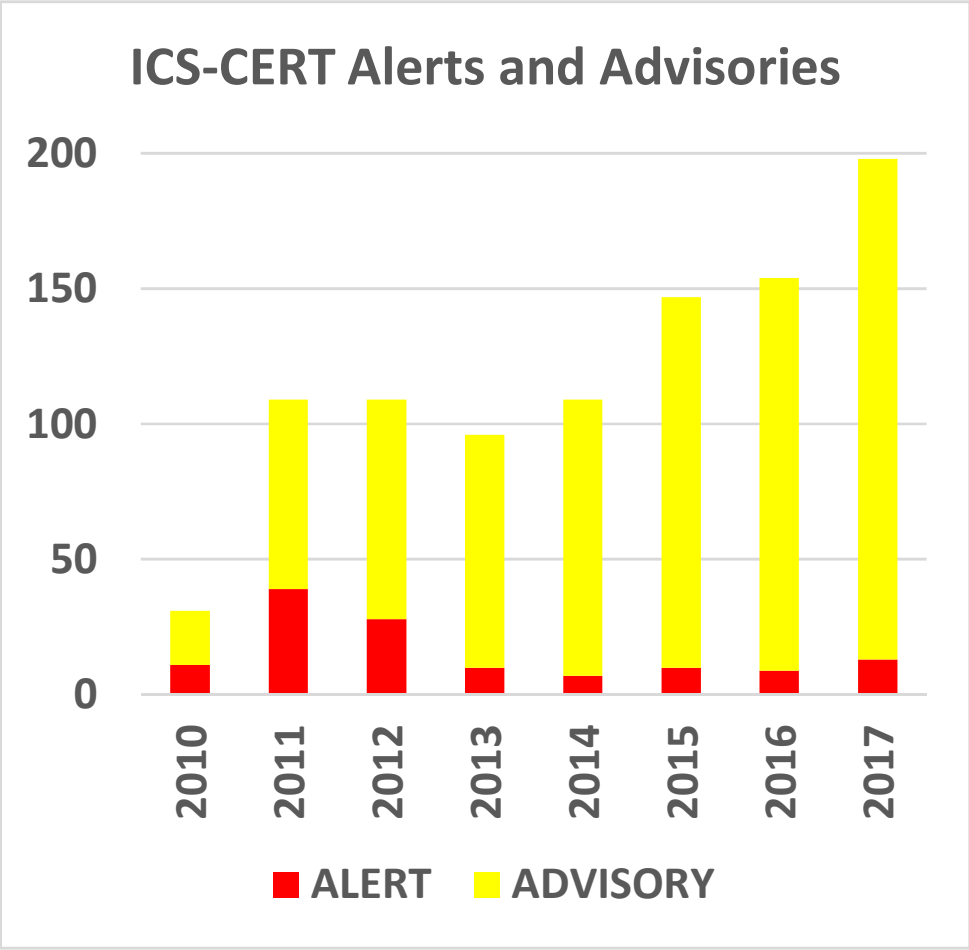


Cybersecurity risks

People → Process → Technology

- Risks moving from IT to OT
- Expanding vulnerabilities and exploits
- Move from obscurity to exposure and solution
- Improved support from vendors
- Improved support from agencies
- Improve standards
- Anticipated flood of risk from IOT
- Busy first 2 months of 2018

ICS-CERT issued 30 alerts and advisories
Malware – 97 updates (Trend Micro)
Microsoft - 173 security updates
Mitre/NVD issued 2,400 new CVEs



People → Process → **Technology**

Dependant Technology Risks

Unexpected dependency on availability/integrity of data or functionality e.g.

- GPS positioning data
- Internet time service/NTP
- Software support expiry (e.g. XP, SaaS)
- PKI certificate validity (revocation, expiry, access)
- Plethora of hidden interfaces (USB, Bluetooth, WiFi, NFC, …)
- Others?????

People → Process → **Technology**

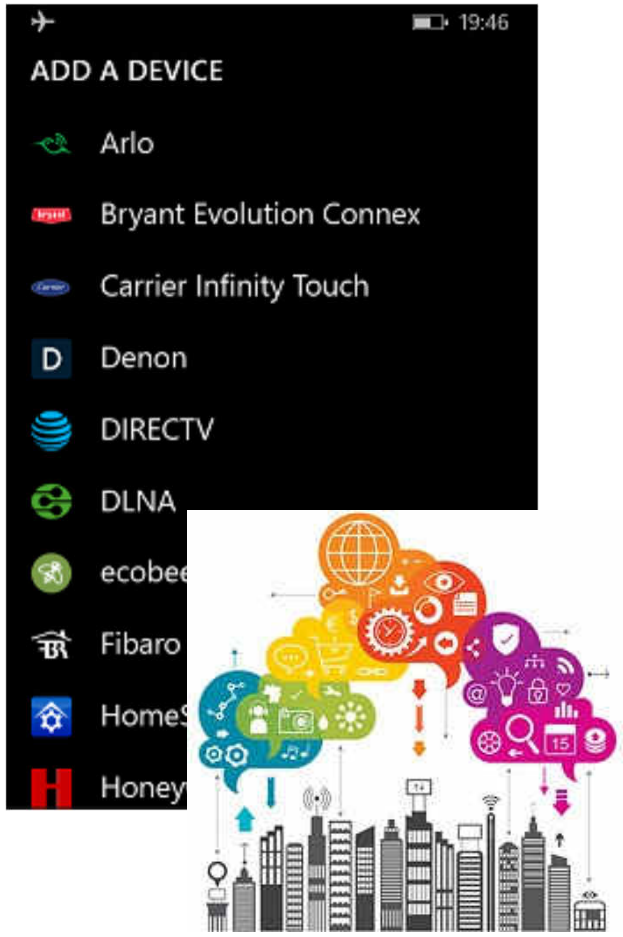
Disruptive Technology Risks

- Internet of Things
  - Driven by cost and market entry advantage
  - IoT easily turned into zombie botnets for DDOS
  - Unproven safety and security
- Pro-innovation bias (coolness conquers caution)
  - Driven by marketplace and quick reward
  - Risk often dumped on unsuspecting society
  - Causes issues with available competence, testing and safety assessment
  - Moved into main stream before proven

Cognitive technology risks

People → Process → **Technology**

- Home Automation
  - Google Now, Siri, Cortana, Amazon Echo,
- Image recognition -False positive and negative risks
- Edge Intelligence - Divided responsibility/authority◊
- Machine/Deep learning vulnerabilities
  - Proven exploits against Artificial Intelligence*
  - Hidden negative training risks
  - Protection of learned memory from attack

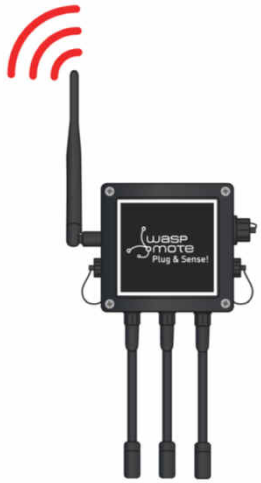


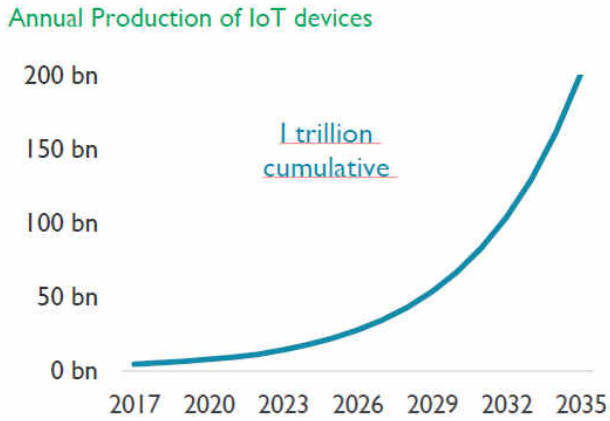
◊TBA ISO/IEC 30141:ED1 Information technology - Internet of Things Reference Architecture (IoT RA)

*I. Evtimov et al, 2017 , "Robust Physical-World Attacks on Deep Learning Models"

Edge intelligence - perfect match or perfect storm?

- Information Technology
  - Internet of Things (IoT)
  - Software as a service, Infrastructure as a service
  - DEVOPS methodology (integrated development/operation)
- Cognitive Technology
  - AI cloud platforms e.g. Microsoft Azure, ARM
  - Deep Learning techniques e.g. IBM
  - Edge technology/OS– e.g. ARM Mbed
  - Internet centric
  - Currently only deployed in industrial system monitoring

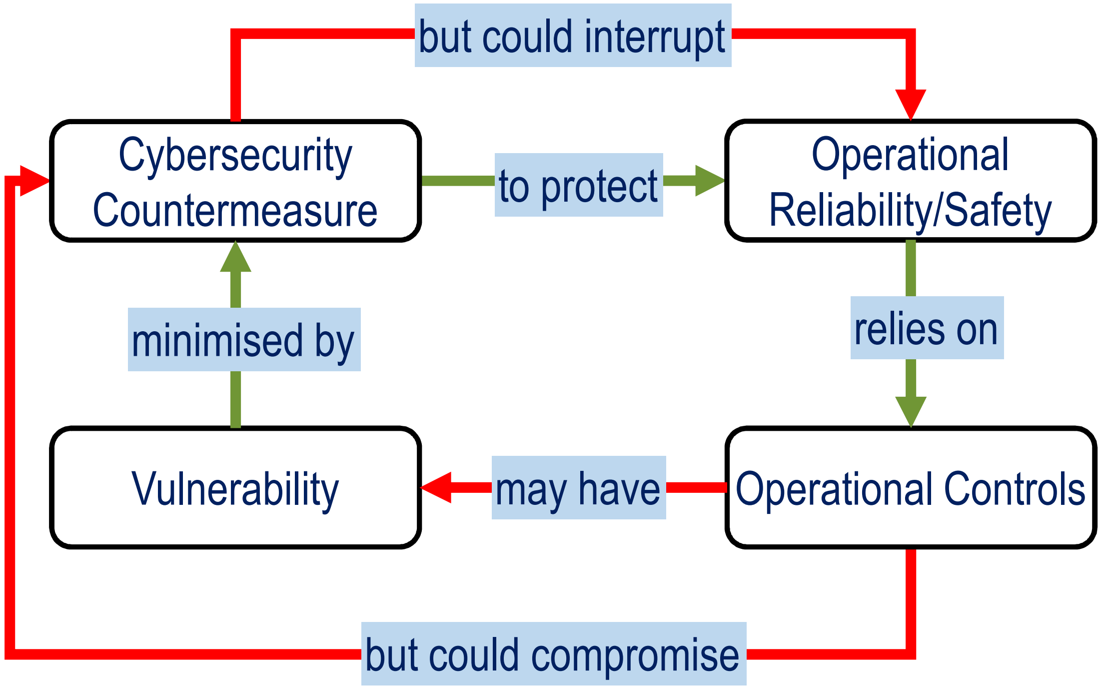




New JTC1-SC41- ISO/IEC 30141 ED1 Internet of Things Reference Architecture (IoT RA)

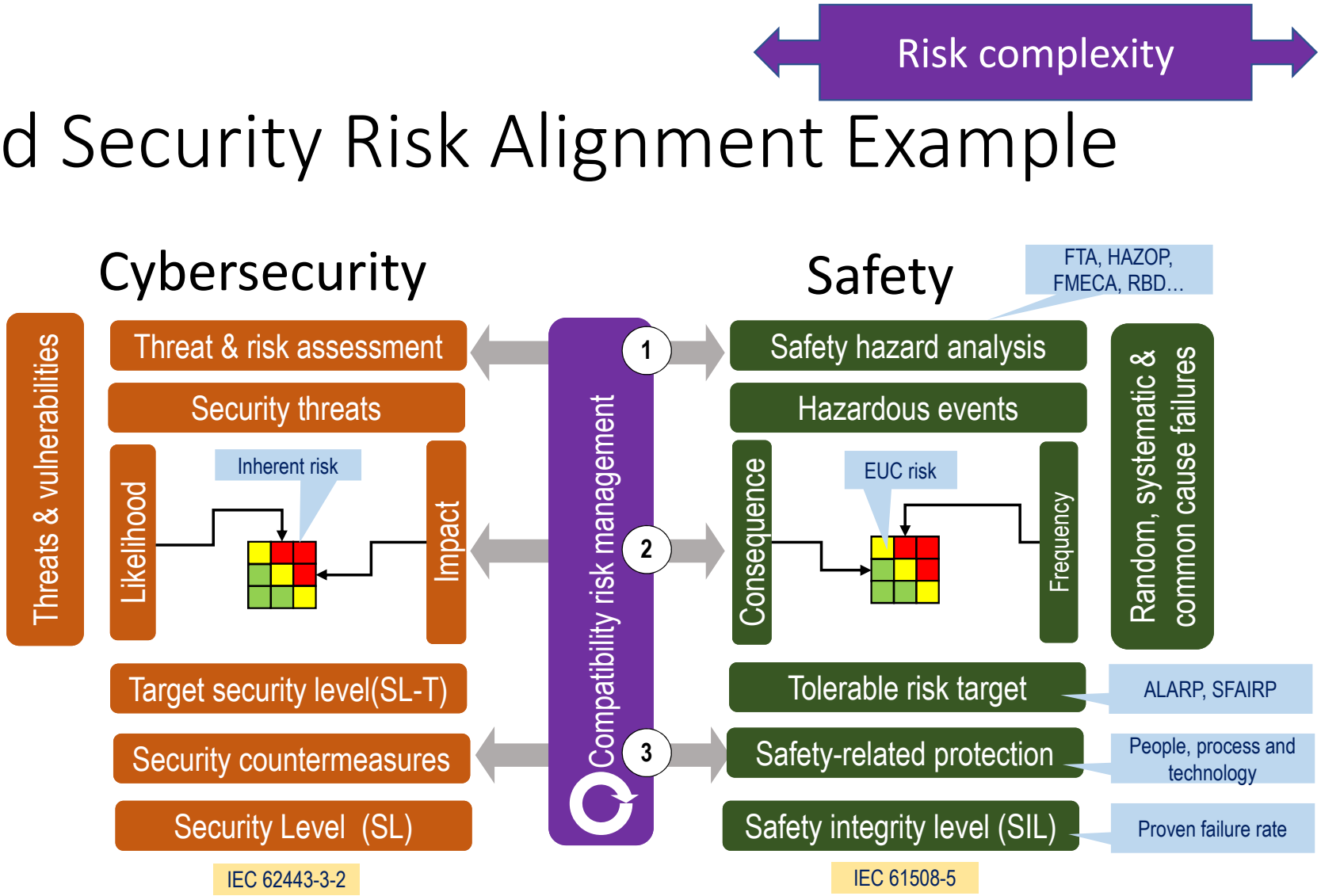
Risk Control Compatibility

- Conflicting control conundrum
- Safety-security principles
    - Safety must be secured
    - Safety controls must be secure
    - **Security controls must be safe**
- **Controls may risk the very thing we're trying to protect**
    - e.g. Germanwings flight 9525



Safety and Security Risk Alignment Example

1. Align context
2. Associate impacts
3. Harmonize controls



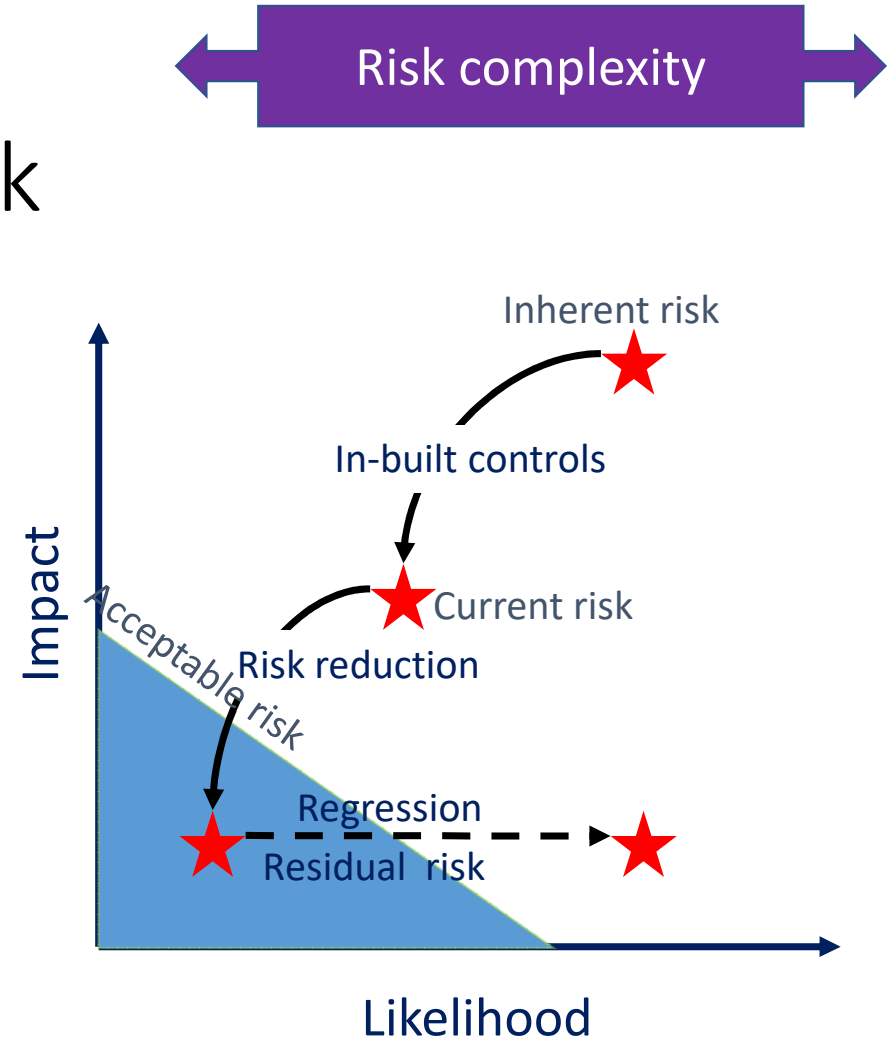
Risk complexity

Cybersecurity risk and regulation?

- Regulation in place for privacy (AU Data Protection, EU GDPR)
- SFAIRP/ALARP
  - Cybersecurity, duty of care and diligence
  - How far is reasonably practical to stop all exploits?
  - Consequential morbidity risk?
  - Cyber event causation - foreseeability
- Critical Infrastructure Cybersecurity
  - EU and UK considering applying penalties (NIS, CPNI)
- Regulatory standards?
- Impact of AS 7770:2018 Rail Cyber Security and other regulatory and industry standards?

Addressing cybersecurity risk

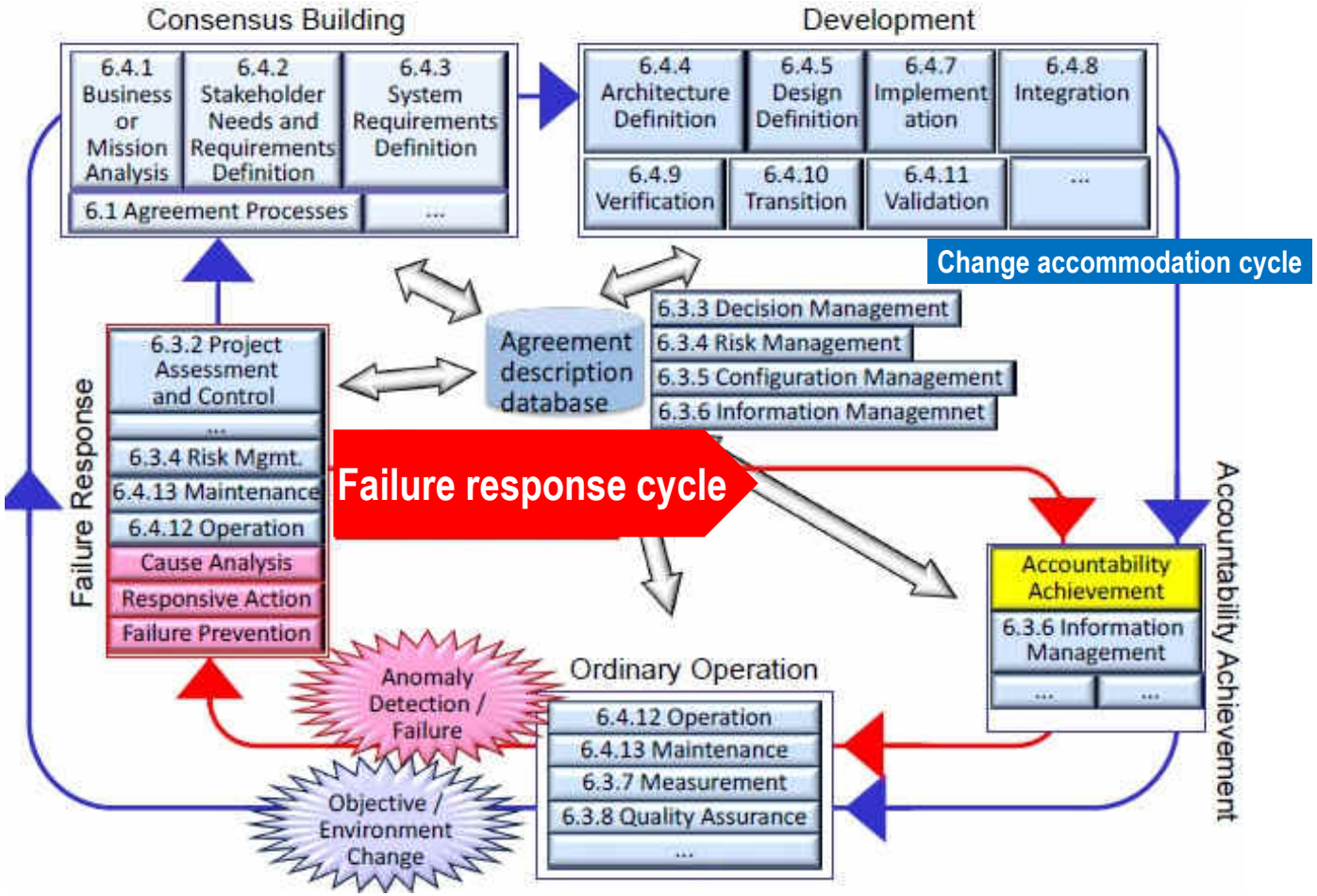
- Improve risk coverage
  - Broad context establishment
  - Risk cooperation across domains
  - Risk communication across domains
  - Address cognitive biases
- Minimise risk regression
  - Change management review
  - Lifecycle risk review
  - Address evolving vulnerability exposures
- Allow for nondeterministic likelihood
  - Rely on multiple layers of separation
- With cybersecurity, there is no real norm…



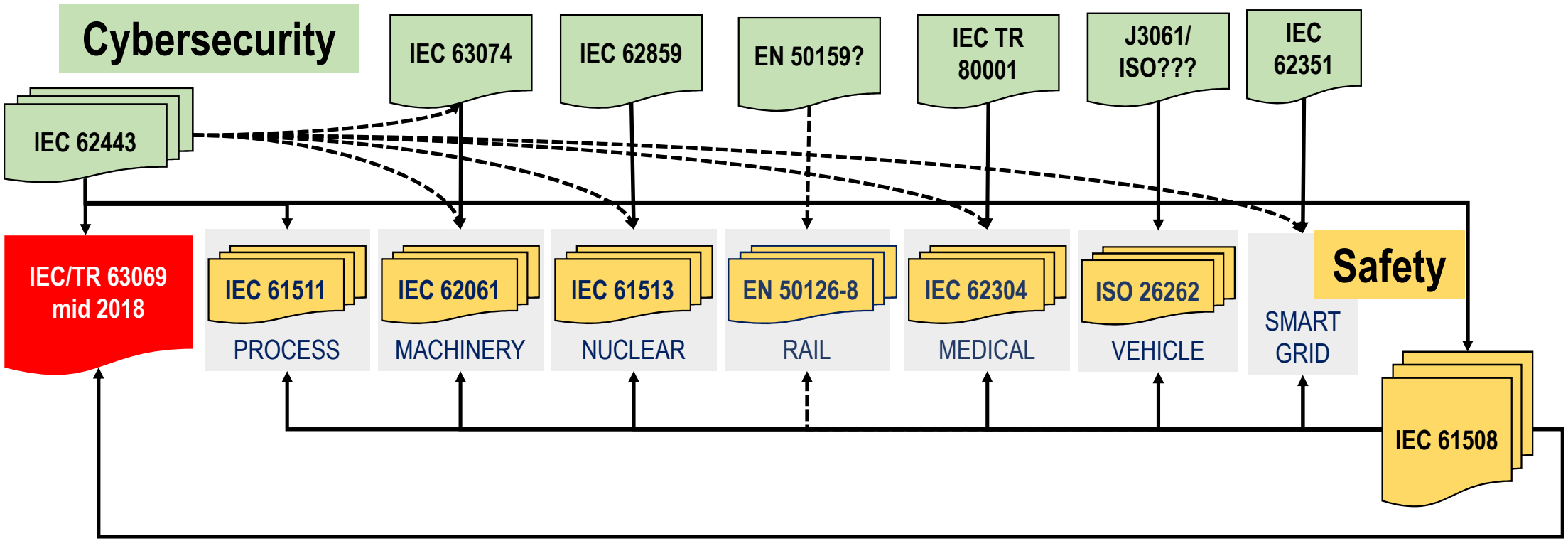
Risk complexity

Keeping connected risk under control

- As entanglements change so does risk
- Continuous review cycle needed
- Possible method
  - Dependable Engineering for Open Systems (DEOS) Life Cycle Model (IEC 62853) may support
  - Failure response cycle



Safety-Security Standards example



IEC DTR 63069 Plan

Framework for functional safety and security

- 2017-08-04 65/678/CD (draft IEC TR 63069) published
- Feb 2018 CD1 comments resolved
- June 2018 DTR and CC published
- 2018/19? IEC TR 63069 ED1 to be published

Liable to change until published

IEC TR 63069 preview

- Title: Framework for functional safety and security
- Objective
  - ..reconcile risk-based paradigms of safety and security standards to provide appropriate resilience and protection..
- Scope
  - common application of IEC 61508 and IEC 62443 in the area of industrial process measurement, control and automation
  - may apply to other industrial sectors where IEC 61508 and IEC 62443 are applied
- What it isn't
  - Detailed cybersecurity or safety standard
- Who is it for
  - asset owners, system integrators, product developers and suppliers, service providers, relevant authorities

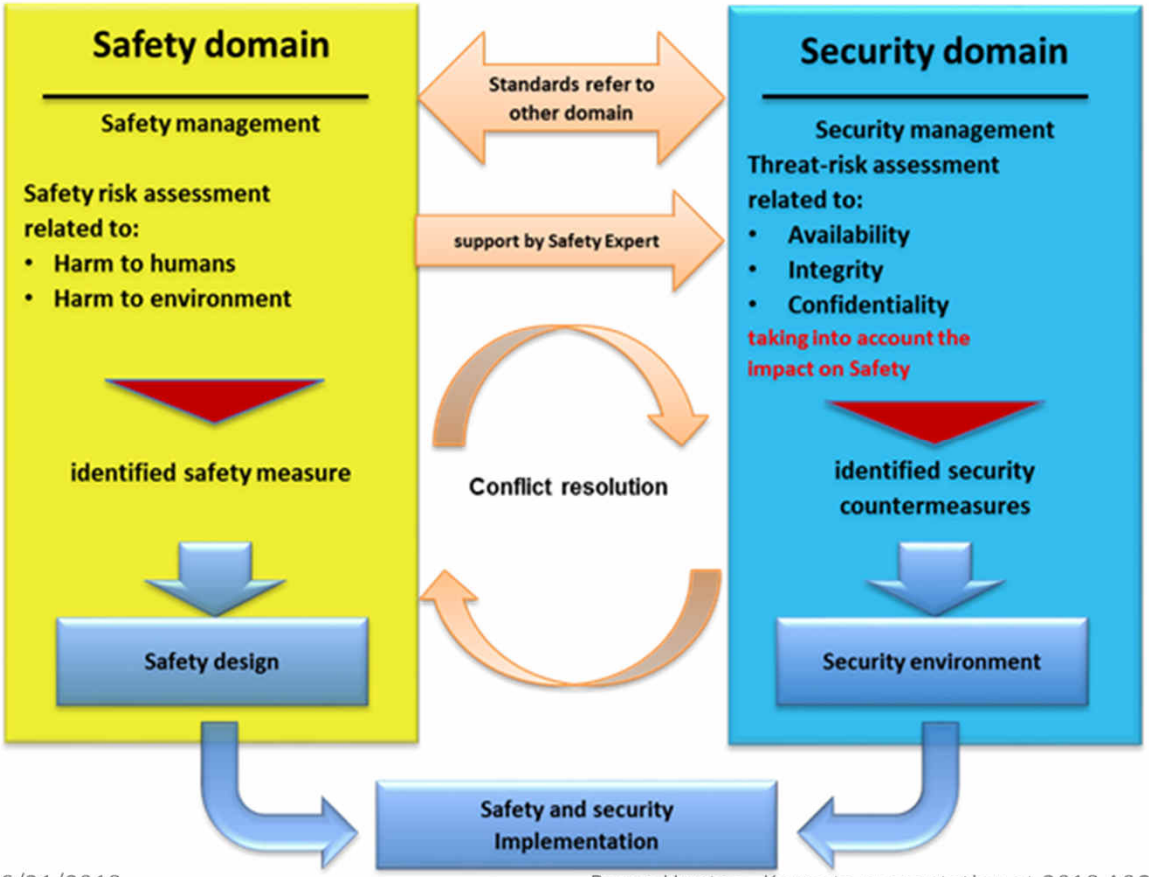
Liable to change until published

IEC TR 63069 Concepts

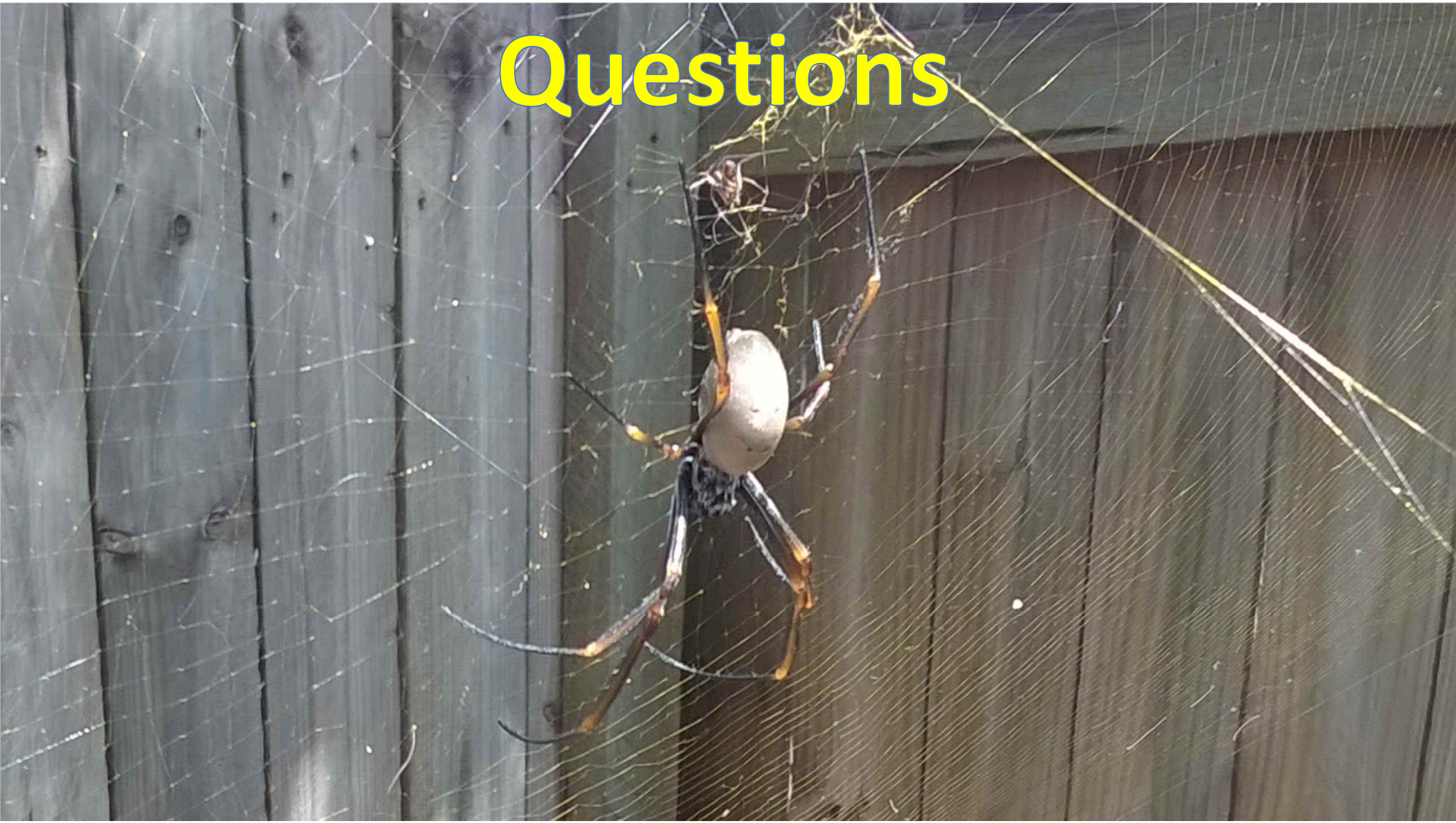
- Does NOT specify safety or security requirements
  - IEC61508 and IEC 62443 do this
- Interpretation of safety and cybersecurity terms
  - Where they differ
- Security context in relation to safety - Guiding Principles:
  - 1: protection of safety implementations;
  - 2: protection of security implementations; and
  - 3: compatibility of implementations.
- High level and lifecycle recommendations
- Risk assessment considerations
- Security application in relation to safety
- Coordinated incident readiness and response

Liable to change until published

IEC DTR 63069
Safety/security lifecycle view



Liable to change until published


Questions

References - standards

- IEC 61508: 2010, “Functional safety of electrical/ electronic/ programmable electronic safety-related”
- IEC 62443, “Security for industrial automation and control systems”
- Proposed IEC/TR 63069 Ed. 1.0 “Framework for functional safety and security”
- AS 7770:2018 Draft, “Rail Cyber Security,” RISSB, 2018
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) 2014
- SP 800-160, Systems Security Engineering
- ISO/IEC 30141 ED1 (stability date 2023) Information technology - Internet of Things Reference Architecture (IoT RA)

References – cybersecurity

- K. Johnson, “Exposing the Fallacies of Security by Obscurity, Full Disclosure,” ISACA Journal, vol. 5, 2017.
- US Department of Homeland Security, “The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT),” [Online]. Available: https://ics-cert.us-cert.gov [Accessed 6 February 2018]
- B. Johnson, C. Dan, M. Krotofil, D. Scali, N. Brubaker and C. Glyer, “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure,” 14 December 2017
- Austroads and National Transport Commission – “Australian guidelines for automated vehicle trials”

References – Artificial Intelligence

- Future of Humanity Institute, University of Oxford et al – “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation”
- Trend Micro Forward-Looking Threat Research (FTR) Team – “Cyberattacks Against Intelligent Transportation Systems”
- UC Berkely – “Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning”
- Evtimov,I et al “Robust Physical-World Attacks on Deep Learning Models”
- IEC White Papers – “Edge Intelligence”, “Internet of Things: Wireless Sensor Networks” http://www.iec.ch/whitepaper/
- ARM IOT https://pages.arm.com/iot-solutions-for-dummies.html

References – human behaviour

- Kahneman, Daniel – “Thinking, fast and slow”
- Ip, Greg – “Foolproof, why safety can be dangerous and how danger makes us safe”
- European Aviation Safety Agency. – “Task Force on Measures Following the Accident of Germanwings Flight 9525”
- Slovic, Paul - "Perceptions of risk“
- Anderson, Jack – “The Wall is the Wall: Why Fortresses Fail”
- Taleb, Nassim Nicholas – “Antifragile – things that gain from disorder”