

Implementation and application of an IT-security process in nuclear facilities

Harald Schugt, EnBW Kernkraft GmbH



Introduction

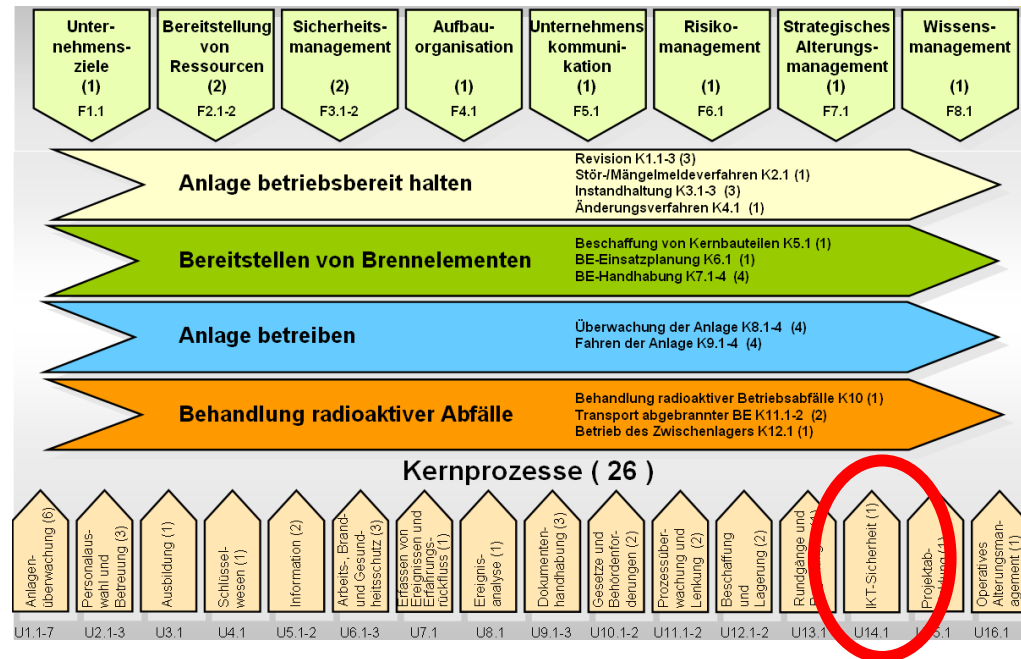
- Harald Schugt
- IT Security Manager in the physical protection department at EnKK NPP Neckarwestheim I and II
- Member of IAEA Working Group „Computer security at nuclear facilities“
- Working and project experiences in I&C, process information systems, computer networks
- In 2006 implementation of an overall IT security process on the site



Implementation of an ISMS at a NPP

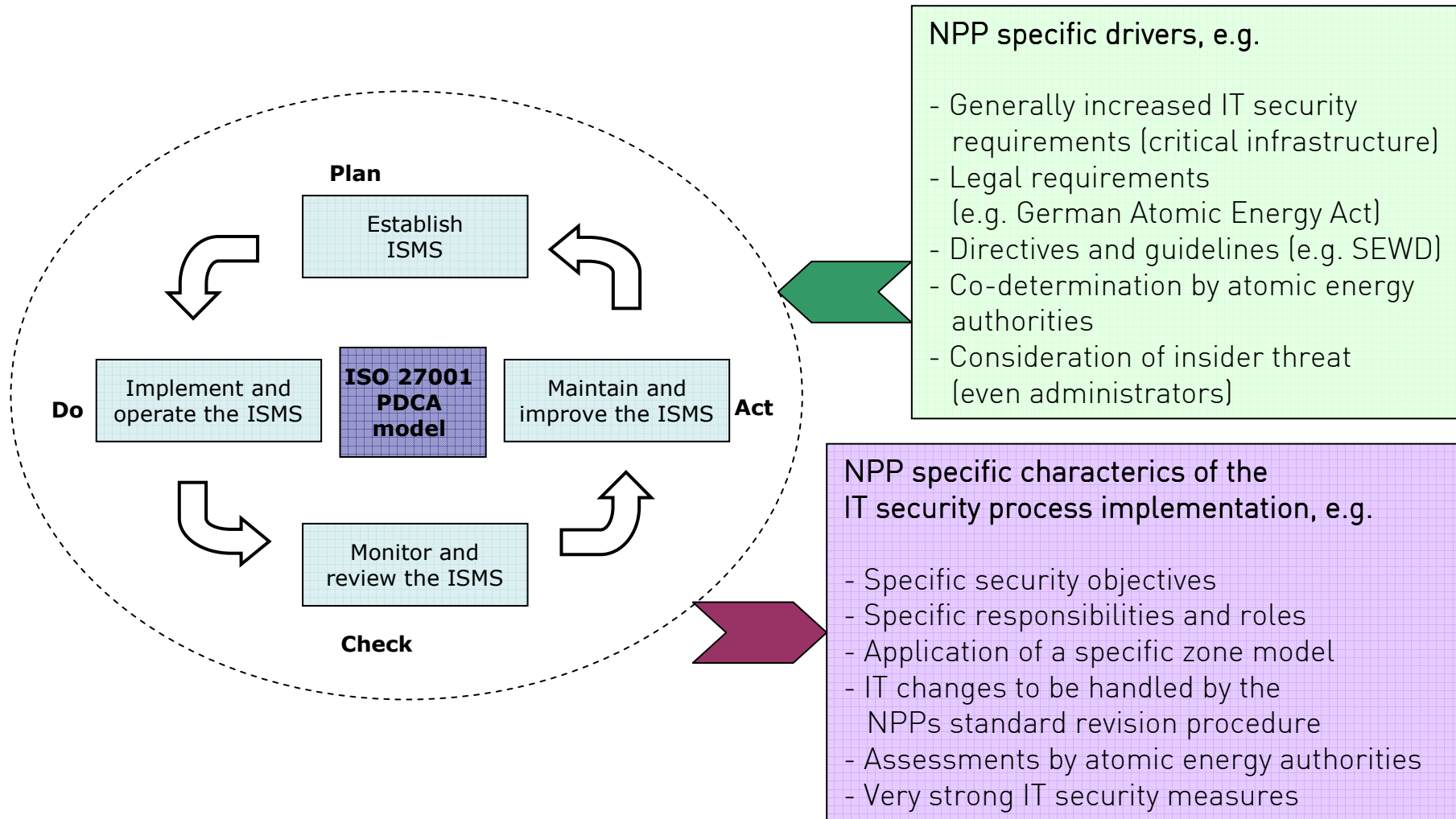
- ISMS is part of the plant's overall integrated management system (SMS)

- ISO 9000 based
- ~ 25 core business processes
- ~ 30 supporting processes (e.g. IT security)

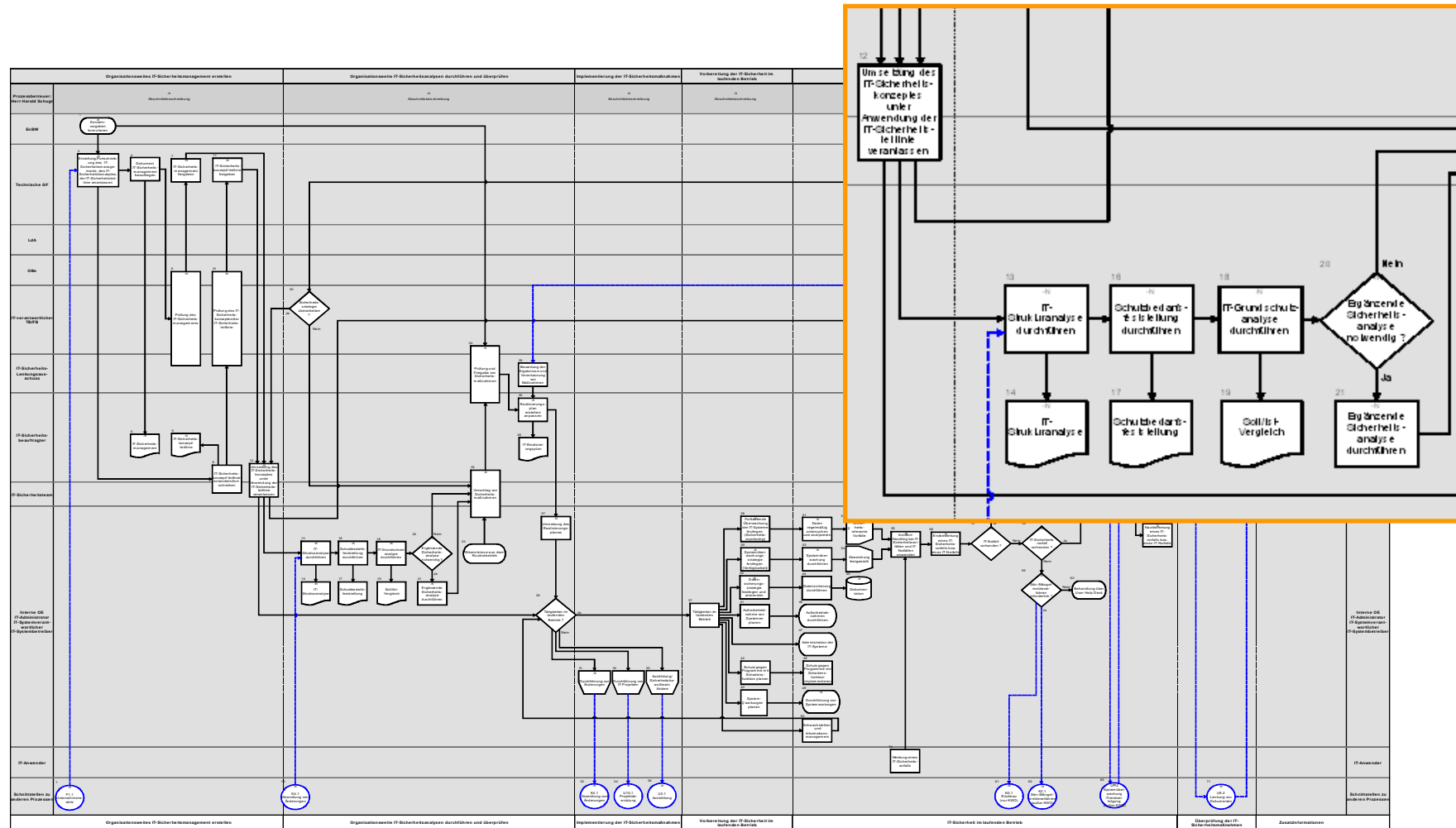


- Indicators to monitor process targets, e.g.
 - Rate of elimination of IT security related audit findings

Implementation of an ISMS at a NPP



Implementation of an ISMS at a NPP



Important standards and directives

- ISO 27001, BSI Standards 100-1 (Management), 100-2 (Basic protection), 100-3 (Advanced risk analyses)
- Richtlinie für den Schutz von Kernkraftwerken mit Leichtwasserreaktoren gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD)
- Security of Information and Instrumentation at Control Systems at Nuclear Facilities (Draft: IAEA Technical Guidance)

NPPs IT security objectives

IT security objectives at NPPs

Traditional information security objectives

- Confidentiality
- Integrity
- Availability

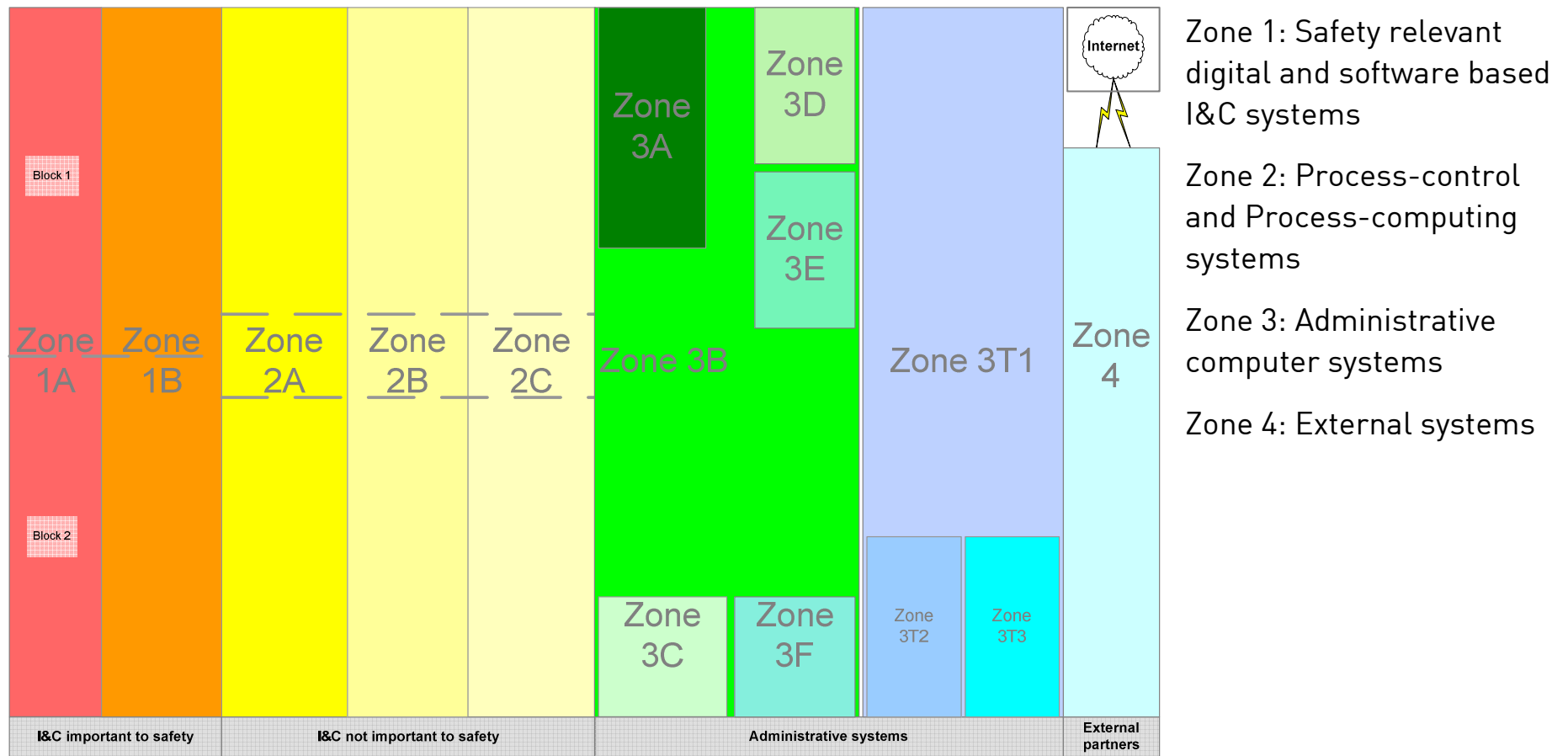
NPP specific IT security objectives

- Absence of feedback or reaction of an IT system to safety related (IT or Non-IT) systems
- IT systems must not contribute to malicious attacks endangering nuclear safety

Requirements concerning an IT security zone model

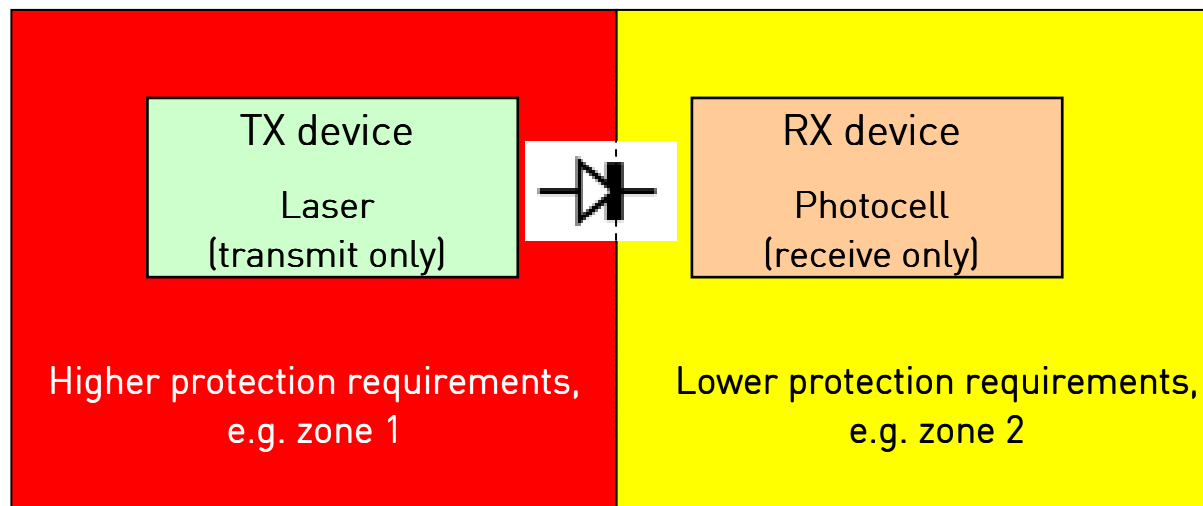
- Zone = Logical grouping of IT systems
 - Similar importance concerning safe and secure operation of the plant
 - Similar protection requirements
 - Sub-zones to demarcate one area from another functionally or to meet different protection needs within one zone
- Defined person is responsible for all IT systems of a zone
 - Individual head of department
- Communication across zones boundaries are strongly regulated by policies and technical decoupling mechanisms
- Communication restrictions rise by the demands of protection levels of zones

Example implementing an IT security zone model

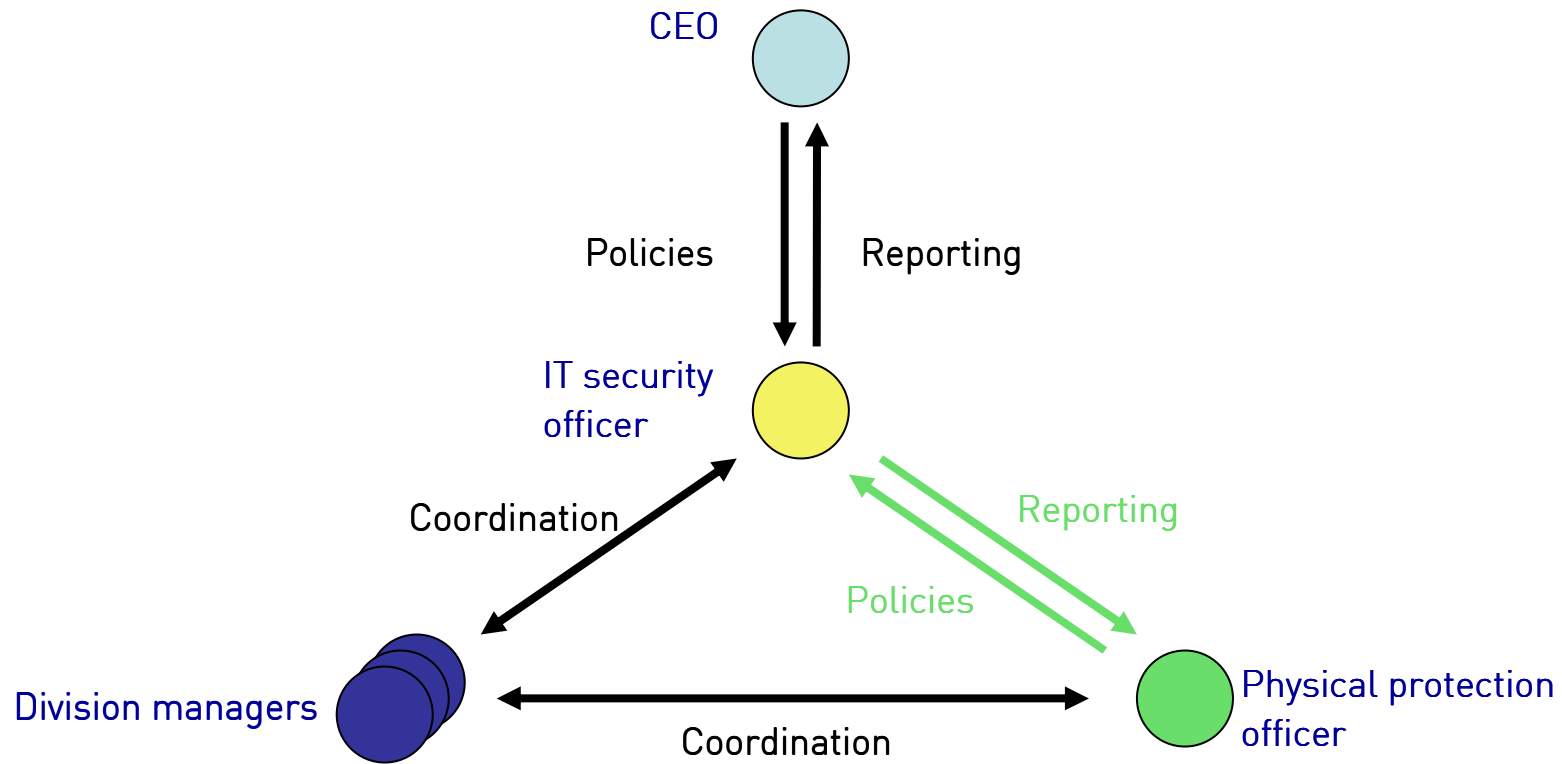


Example implementing an IT security zone model

- Example:
Decoupling zone 1 from zone 2 by a physical device ensuring strict one-way communication



Example IT security organisation



Example IT security organisation

- IT security steering committee
 - Strategically consulting and enhanced development of the IT security process
- IT security team
 - Inter-divisional coordination of IT security
- Information owner / process owner
 - Defines the protection needs of data and IT-systems

Examples of IT security measures in NPPs

- 4-eyes-principle accessing highly protectable server rooms and racks
- 4-eyes-principle administrating highly critical IT systems
- Strong physical protection of server rooms and administration rooms
- Extensive logging and alarming mechanisms (software, racks, rooms)
- Well defined IT-emergency procedures
- Adoption of software, e.g. integrity checks and encryption
- Any IT change must be handled using the NPPs standard revision procedure, often accompanied by regulator and external assessors

IT security and I&C systems

- Still today I&C system design and software development is focused on functional aspects, in particular reliability and availability
- IT security measures, e.g. encryption, hardening or strong authentication, are typically not implemented
- Vendors still consider I&C systems as fully isolated
- Requirements interconnecting I&C to other systems are growing permanently



Conclusions

- Implementing an structured IT security process is a relevant change
- All relevant stuff has to be integrated into this process
- The process has a very broad basis and covers almost all fields of plant activities
- Involved persons need a broad knowledge covering IT, nuclear operations, safety and security
- IT systems are typically not set up “IT security ready” by vendors. In consequence relevant projects have to be supported by the IT security process.