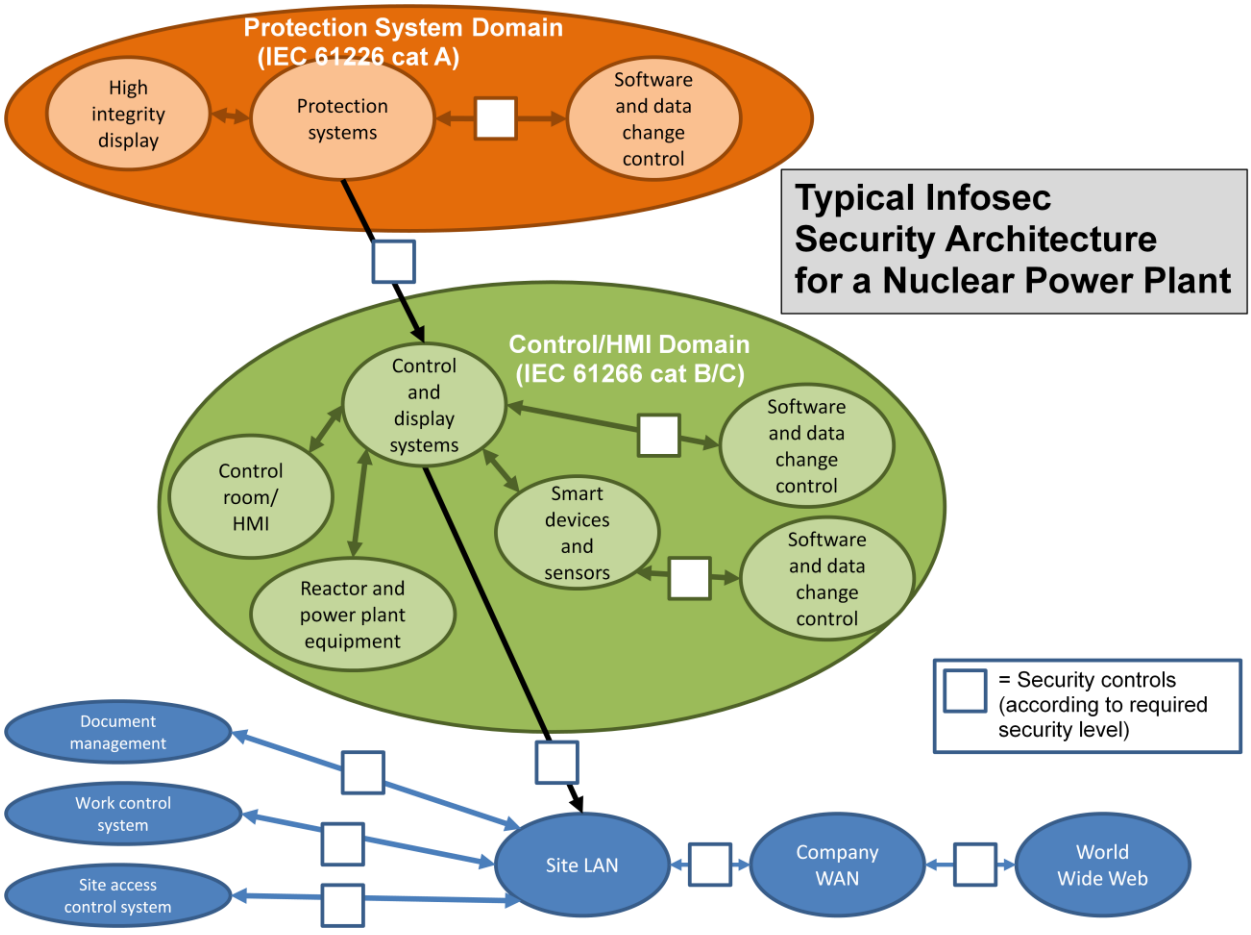
Safety*In*Engineering

Nuclear Plant Information Security – A Management Overview

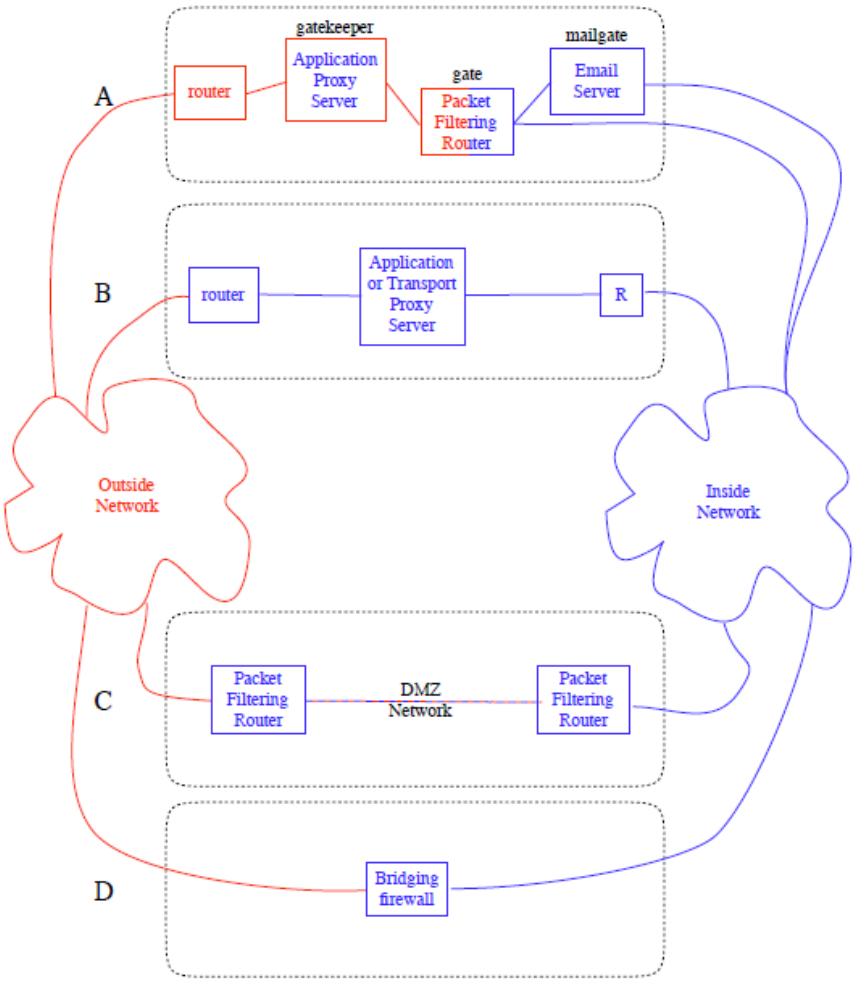


The diagram above is a typical (simplified) Infosec Architecture Model for a nuclear power plant. The fully-developed model would, for example, contain more detail about software development, change controls, firewalls and unidirectional networks. Diversity and separation requirements in nuclear power plants generally mean that nuclear plant systems are already robust against cyber attack.

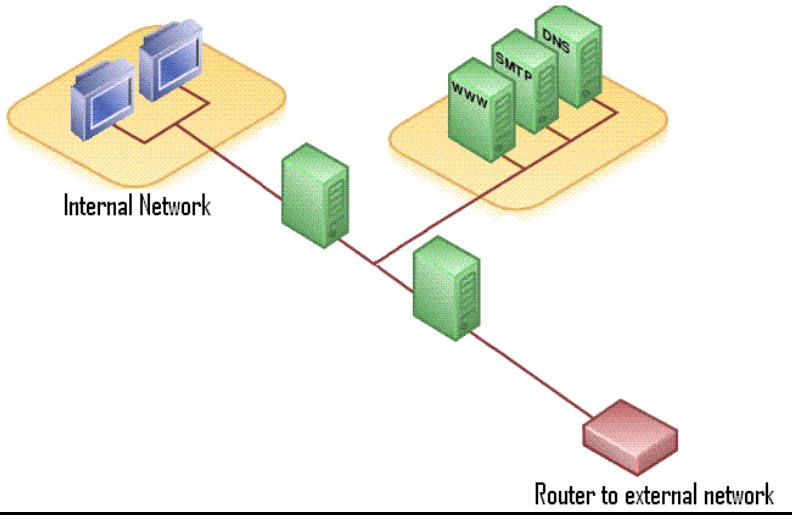
Basic Terminology related to Domain-Based Security

"Domain-Based Security" (DBSy) is a technique developed by Qinetiq Ltd and endorsed by the UK Ministry of Defence for the analysis of information security in plant systems. It requires the IT systems to be analysed by 'domains' as shown in the diagram above so that the different security levels and the key barriers can be identified.

Domain	Logical grouping of systems and people within which information can be freely shared.
Environment	Models of the physical world from where people interact with systems via a *Portal.*
Connections between domains	These define the limits of interaction.
Islands of infrastructure	Single machines or groups of networked machines that operate together to support a business function.
Causeways	Secure connections between Islands.
Infosec Architectural Model	This incorporates both the business functions and the technical world in which they operate, and thus enables the different views of system users, security advisers and developers to be discussed.
Risk	This has three elements: Threat, Vulnerability, and Impact. Controls or countermeasures can be applied to each.
Threat Actor Groups (TAGs)	Internal: Operators, Engineers with high-level access privileges. External: Connected users, Maintenance and Repair, Visitors, Those with wider access, Regulators and security advisers, natural disasters
C, I, A	Confidentiality, Integrity, Availability



Types of Firewall Network



Dual-Firewall DMZ Network Architecture (also called Perimeter Architecture)

Firewall terminology

Data diodes and unidirectional networks	These are the methods of ensuring one-way transmission of information from a higher-security ('trusted') system to a lower-security system, but not vice-versa.
Network layer or packet filter firewalls	Do not allow packets to pass through the firewall unless they match the established rule set. Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).
Applications layer firewalls	Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender). The key benefit of application layer filtering is that it can "understand" certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way.
Proxy firewalls	A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.
Bridging versus Routing firewalls	What is the difference between a bridging ('transparent') firewall and a conventional firewall? Usually a firewall also acts as a router: systems on the inside are configured to see the firewall as a gateway to the network outside, and routers outside are configured to see the firewall as the gateway to the protected network. A bridge is piece of equipment that connects two (or more) network segments together and passes packets back and forth without the rest of the network being aware of its existence. In other words, a router connects two networks together and translates between them; a bridge is like a patch cable, connecting two portions of one network together. A bridging firewall acts as a bridge but also filters the packets it passes, while remaining unseen by either side.

Fig 6 is a flow chart showing the multiple interconnections between the concepts of threat, vulnerability and risk (from IAEA pub 1527).

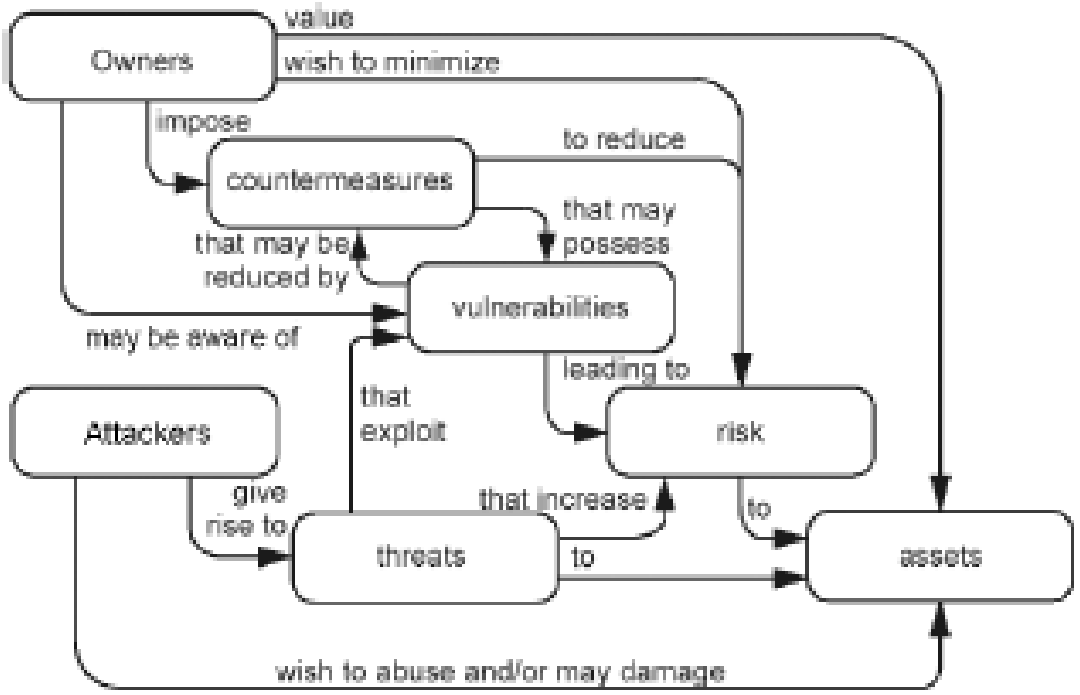


FIG. 6. Security concepts and relationship (adapted from ISO 13335-1 2004 [16]).

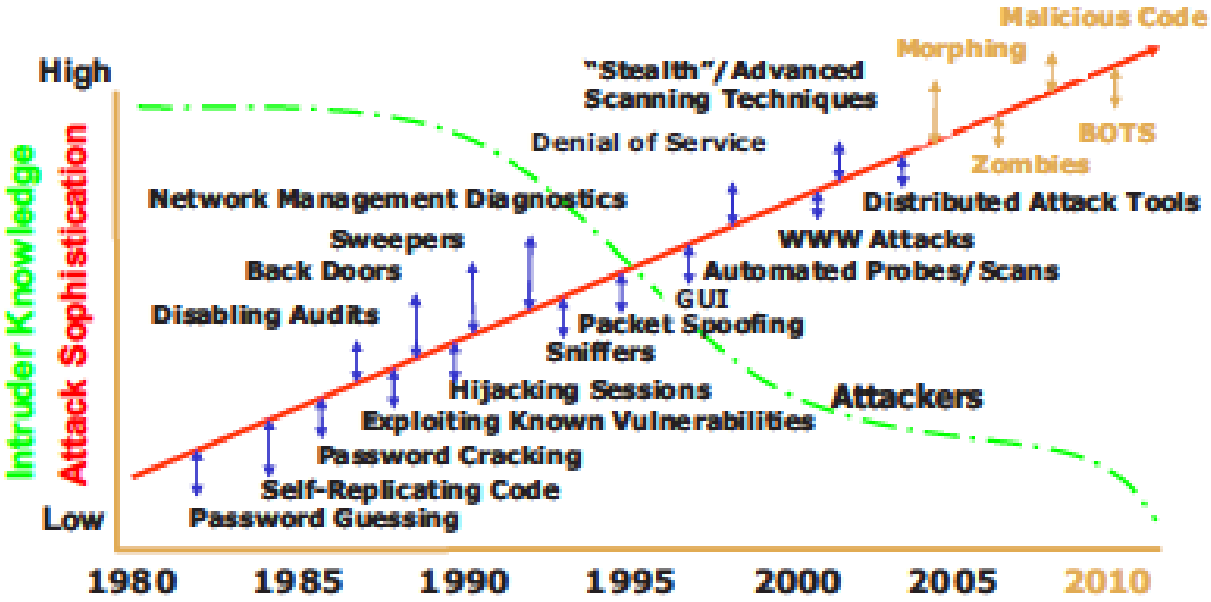


FIG. 7. The increasing complexity of threats as attackers proliferate.[4]

Security classification is in accordance with safety classification, which is done in accordance with IEC 61266. IAEA publication 1527 makes recommendations for minimum countermeasures according to security classification, as follows:

Cat* IEC 61266	**Description**	**Typical functions**	**Possible security level and counter measures (IAEA pub 1527)**
A	Principal role in achieving safety	1. Reactor shutdown/holddown 2. Decay heat removal 3. Containment 4. Essential displays	Level 1: No network data flow of any kind. Strict outward comms only, which excludes handshake protocols such as TCP/IP. No remote maintenance access. Physical access strictly controlled. All data entry is approved and verified.
B	Complementary role to Category A	1. Spent fuel pool cooling 2. Main cooling system isolation 3. Post accident monitoring system 4. Automatic control 5. Monitoring and control of fuel handing	Level 2: Outward one way network data flow from level 2 to level 3 systems only. Remote maintenance access may be allowed on a case by case basis for limited time only. Physical connections must be strictly controlled.
C	Auxiliary or indirect role	1. Monitoring category B functions in post-accident phase 2. Warning of internal or external hazards 3. Functions where operating mistakes could cause very minor radioactive releases	Level 2: Outward one way network data flow from level 2 to level 3 systems only. Remote maintenance access may be allowed on a case by case basis for limited time only. Physical connections must be strictly controlled.
-	(i) Document management, (ii) Work permit and control system, (iii) Access control system		Level 4: Only approved users are allowed. Access to the internet from level 4 systems may be given to users if adequate protective measures are employed. Security gateways are implemented. Physical connections are controlled. Remote maintenance is allowed and controlled. System functions available to users are controlled by access control mechanisms. Remote external access is allowed for approved users.
-	Email		Level 5: Only approved users can make modifications to the systems. Internet access is allowed subject to protective measures. Remote external access is allowed subject to protective measures.

*EdF Energy subdivides Cat B into “Significant Cat B” and “Less significant Cat B”. Systems which fall into Cat C or “Less significant Cat B” can be assessed using DBSy ADVANTAGE. Systems with a higher classification require the full DBSy approach.