



## Secure by Design

**Adrian Prior, MSc CSyP MSyI**

WINS, Ottawa, 20<sup>th</sup> - 21<sup>st</sup> November 2019

**SYSTEMS AND ENGINEERING TECHNOLOGY**



# Format

- UK Government Nuclear Innovation Programme
- What is 'Secure by Design'
- Potential Benefits
- Principles, Tools and Process
- Challenges and measuring success



Secure by Design

# UK Government Programme



Department for  
Business, Energy  
& Industrial Strategy

## Nuclear Innovation Programme

### UK Government ambitions for Nuclear Energy

- Industrial Strategy – Nuclear Sector Deal
- Clean Growth Strategy



*“Nuclear is a vital part of our energy mix, providing low-carbon power now and into the future”*

*“...bring down the costs of nuclear power while maintaining safety by investing in innovation that will help plants to be built to time and budget”*



Around £180 million (~€204 M) of the 2016-21 BEIS Energy Innovation Programme will be invested in nuclear innovation.

# What is Secure by Design?

Secure by Design



## Defining the concept?

- ▶ Building-in security?
- ▶ Build-on security
- ▶ Designing something to be secure by default?
- ▶ Or something else?

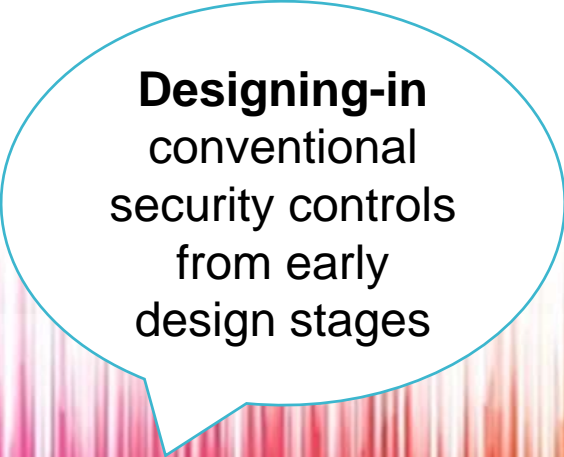


# Security design model 1

**Retro-fitting**  
conventional  
security controls  
in the later  
design stages




## Security design model 2



**Designing-in**  
conventional  
security controls  
from early  
design stages

## Security design model 3



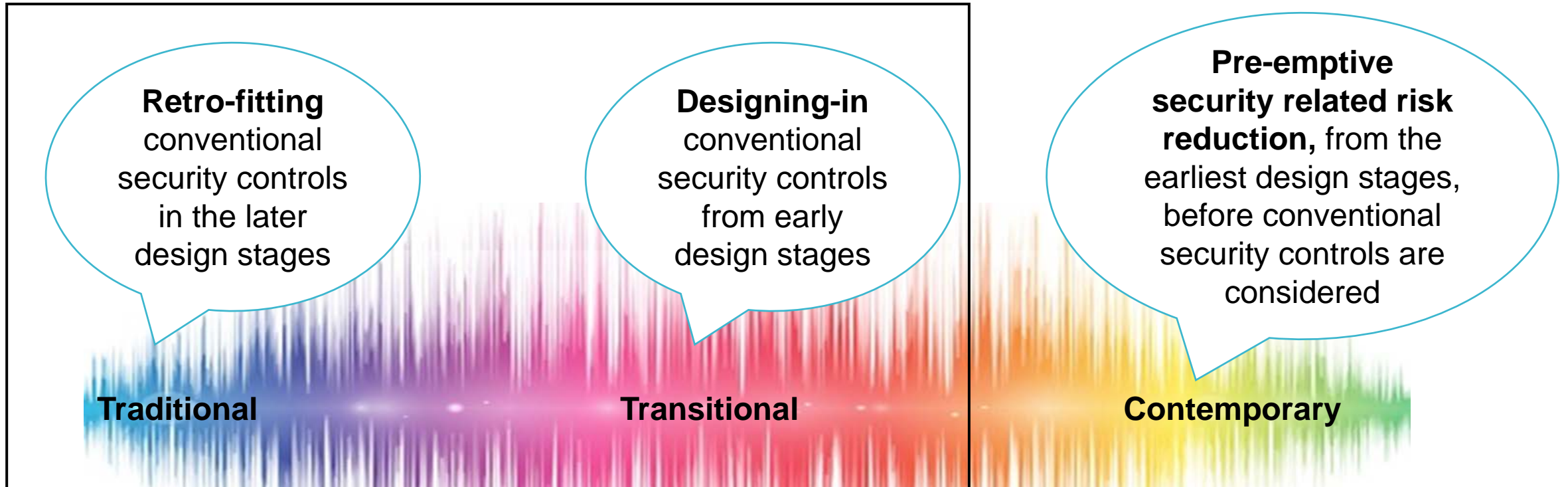
**Pre-emptive security related risk reduction**, from the earliest design stages, before conventional security controls are considered



# Spectrum of security design models

Common approaches to security design

SBD



## Working definition of SBD

- ▶ “...including security within the systems engineering for the facility, thereby reducing security risks at source rather than just relying on physical protection measures.” (WINS, 2014).
- ▶ Concept of extrinsic and intrinsic security measures.
- ▶ Seeking to create *inherent* security through *intrinsic* design features, determined in the earliest stages of design.

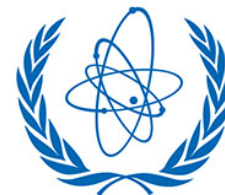


## UK Regulatory expectations and international guidance

- ▶ Key Security Plan Principle (SyAPs, 2017):  
“The underpinning aim should be an inherently secure design, consistent with operational purposes”.
- ▶ ‘Secure by Design’ is an approach that seeks to reduce vulnerabilities [during the design phase] rather than attempting to secure or mitigate them post design”.
- ▶ For a new nuclear facility, the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control.



Office for  
Nuclear Regulation



**IAEA**

International Atomic Energy Agency

*Atoms for Peace and Development*

# Case Studies (Redacted)

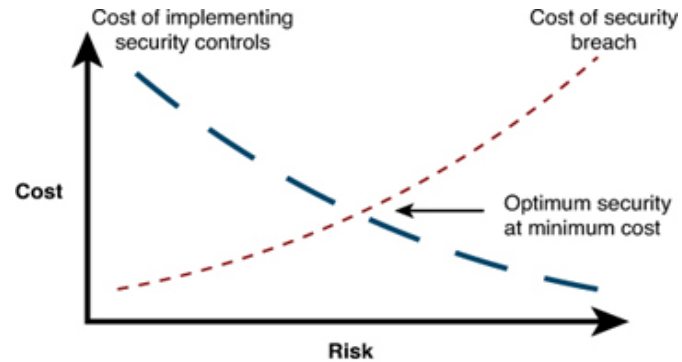
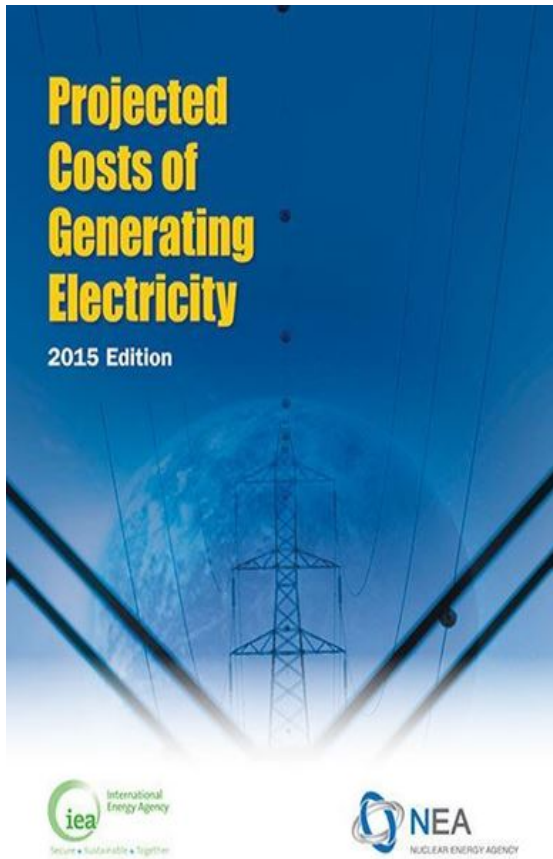
Secure by Design



# Benefits

Secure by Design

# Why is SBD important?

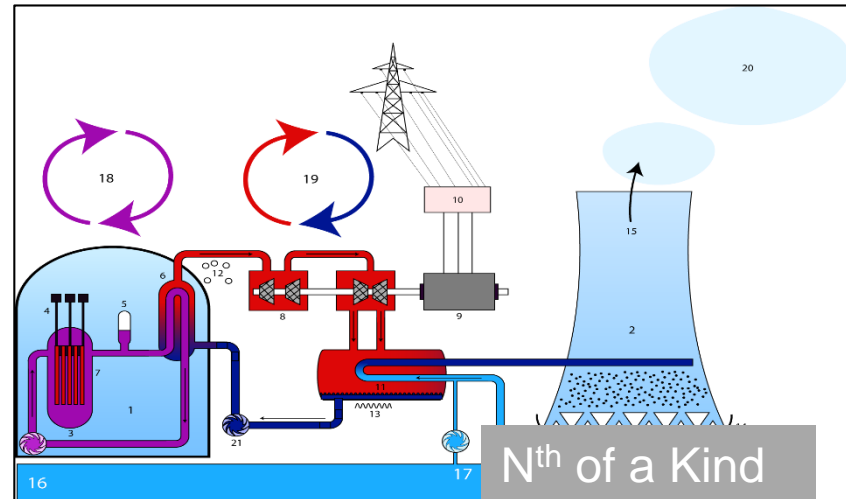


Analysis of cost vs. risk  
Cost of implementing security vs. cost of security breach



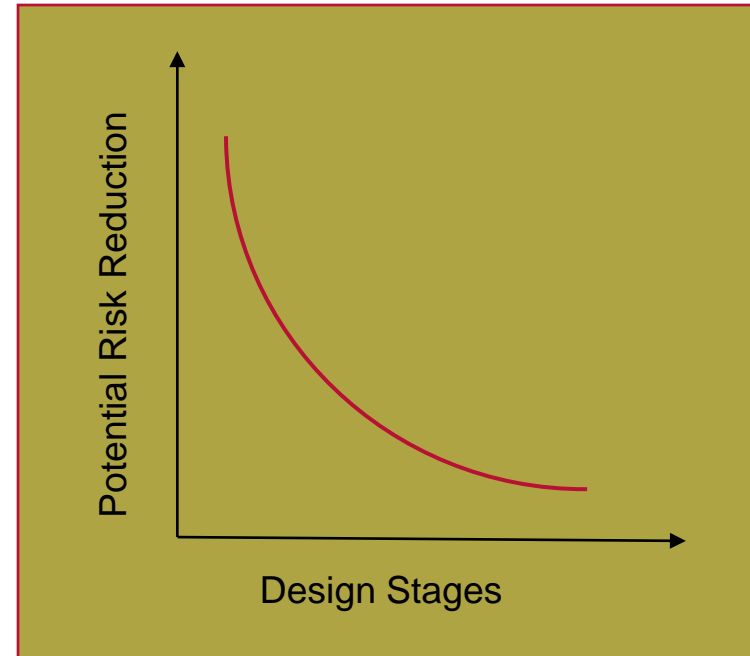


# Potential use cases for SBD



## Potential benefits

- ▶ Reduced expenditure - CAPEX v OPEX
- ▶ Cost effective risk reduction
- ▶ Improved resilience
- ▶ Public confidence
- ▶ Competitive advantage
- ▶ Supports outcome-focused regulation



Security risk reduction curve

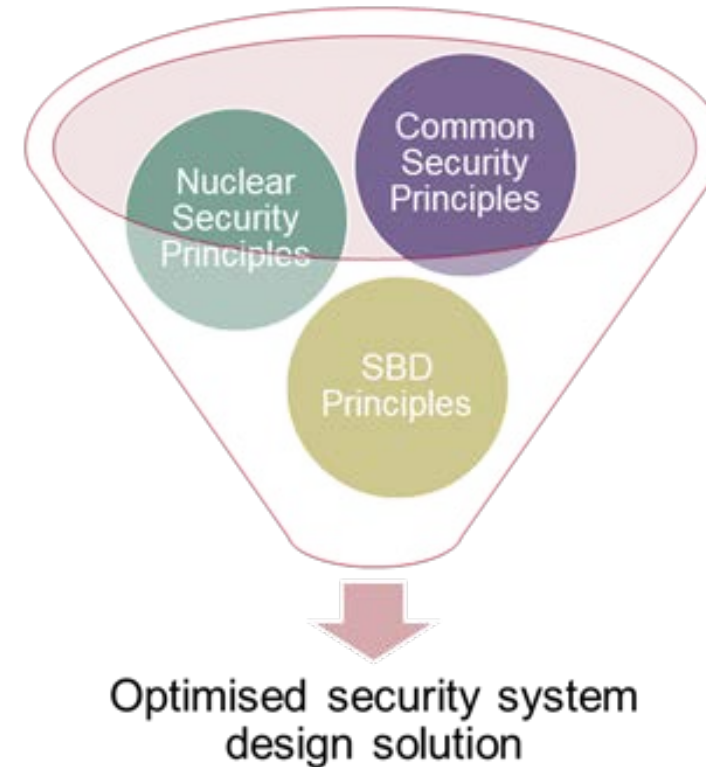


# Principles, Tools and Process

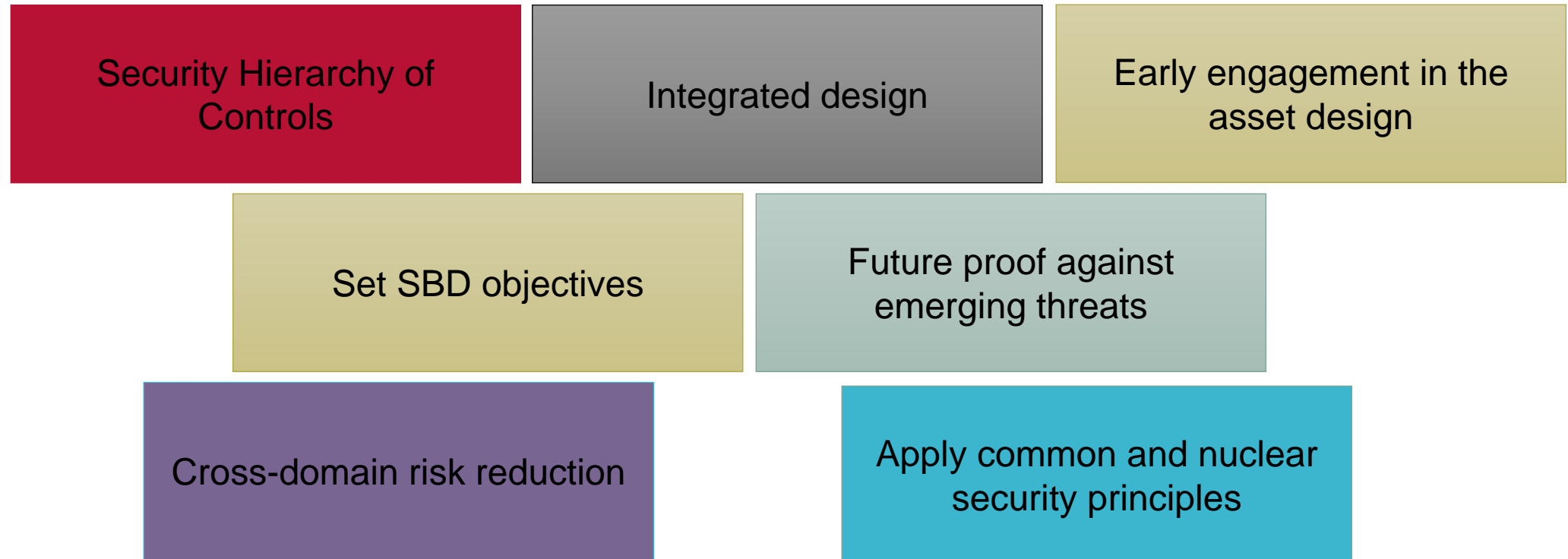
Secure by Design

## Family of Security Principles

- ▶ **Common** security principles
- ▶ **Nuclear** security principles – for PPS and CPS
- ▶ **SBD** principles – application of a SBD approach

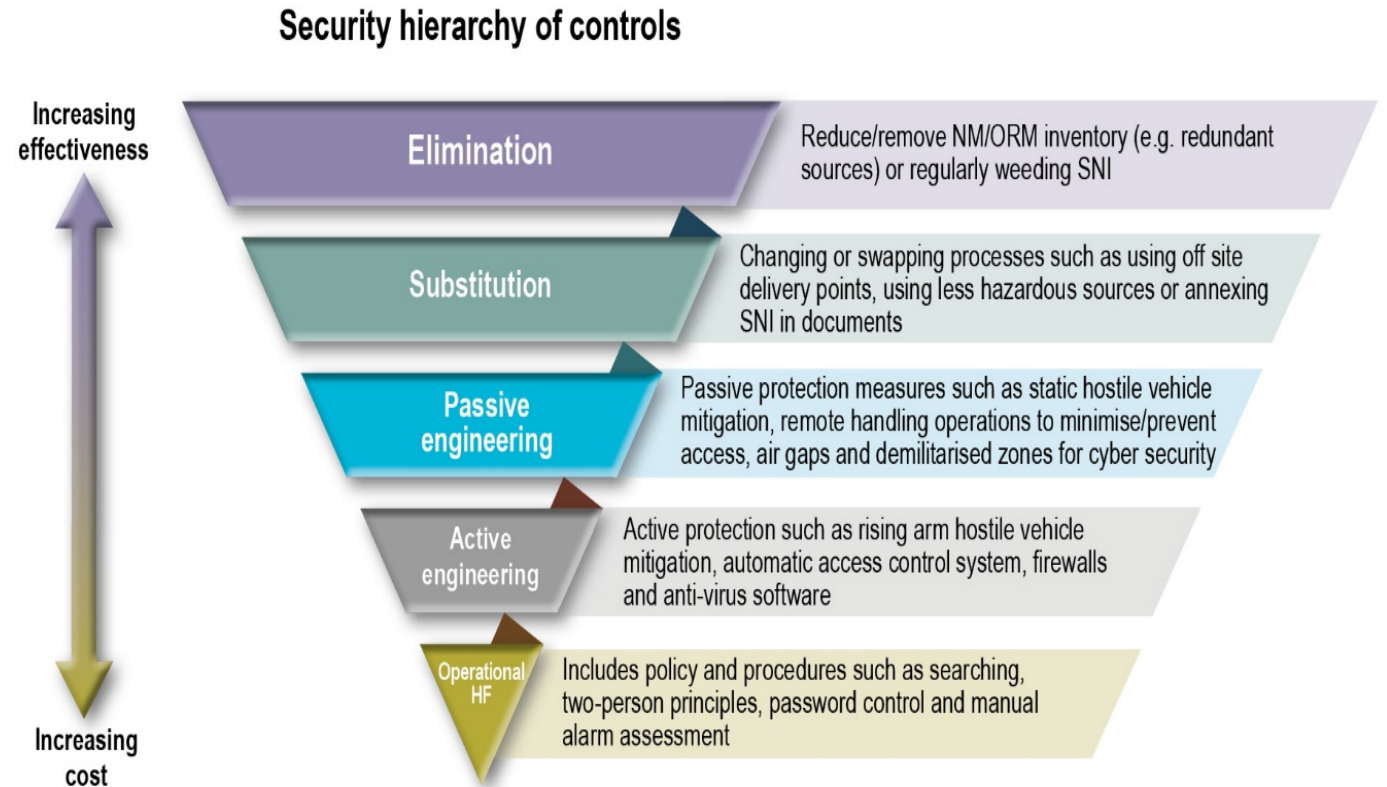


# Candidate SBD Principles



# Techniques and tools

- ▶ Security requirements for design engineers
- ▶ Security of Hierarchy of Controls
- ▶ Threat Analysis – DBT
- ▶ Blast analysis
- ▶ Source term and dispersion analysis
- ▶ Vital Area Identification
- ▶ Extreme load estimations
- ▶ Cost (sacrifice) benefit analysis
- ▶ ALARP concept for security

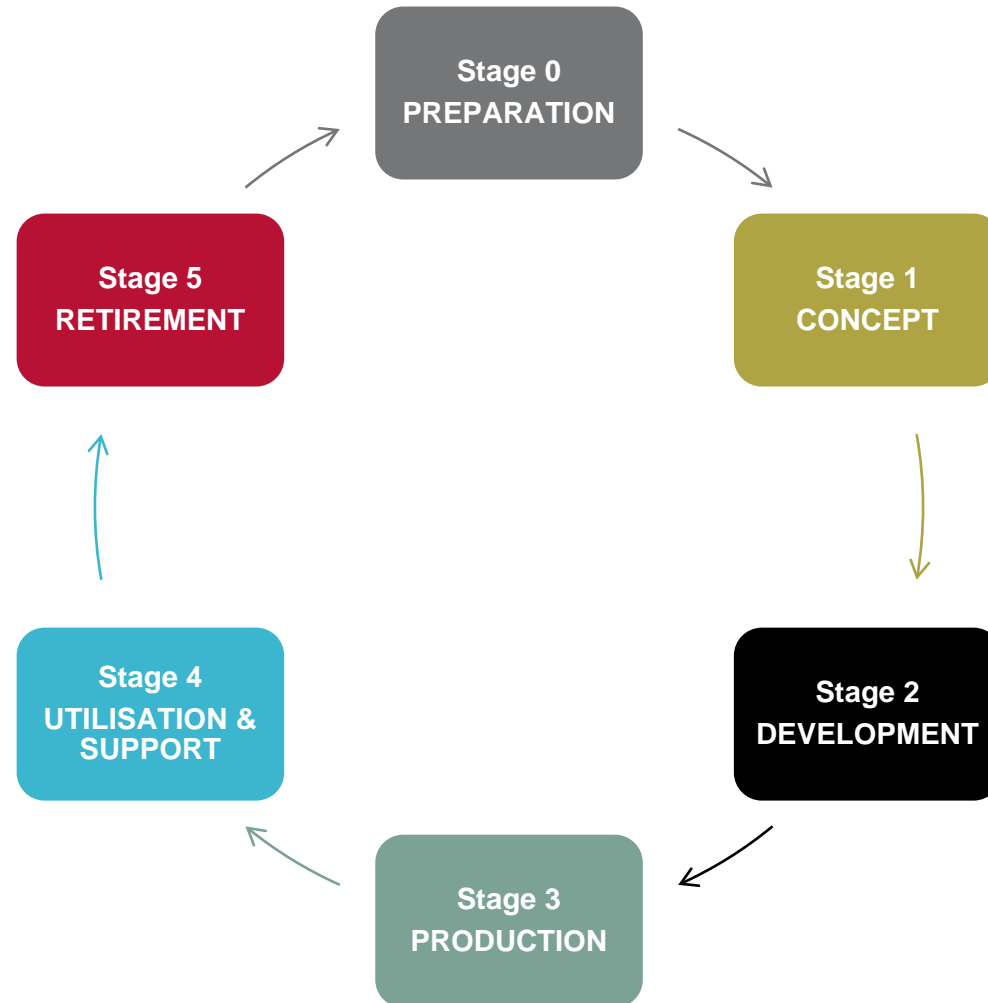




## Utilising Security Objectives

- ▶ Minimise categorisation for theft and sabotage
- ▶ Exploit any viable 'elimination' options first
- ▶ Reduce the number & footprint of potential Vital Areas
- ▶ Exploit opportunity to building-in inherent *delay* - maintain integrity and balance of potential intrinsic barriers (plant structure)
- ▶ Mitigate specific adversary vectors through adaptation of plant design: e.g. aircraft impact
- ▶ Mitigate common construction vulnerabilities: e.g. HVAC voids through barriers
- ▶ Exploit passive engineering solutions, which deliver a security benefit: e.g. passive cooling system
- ▶ Emergency Planning Zone (EPZ) and outer-perimeter alignment
- ▶ Enable safe plant shutdown against defined security challenges

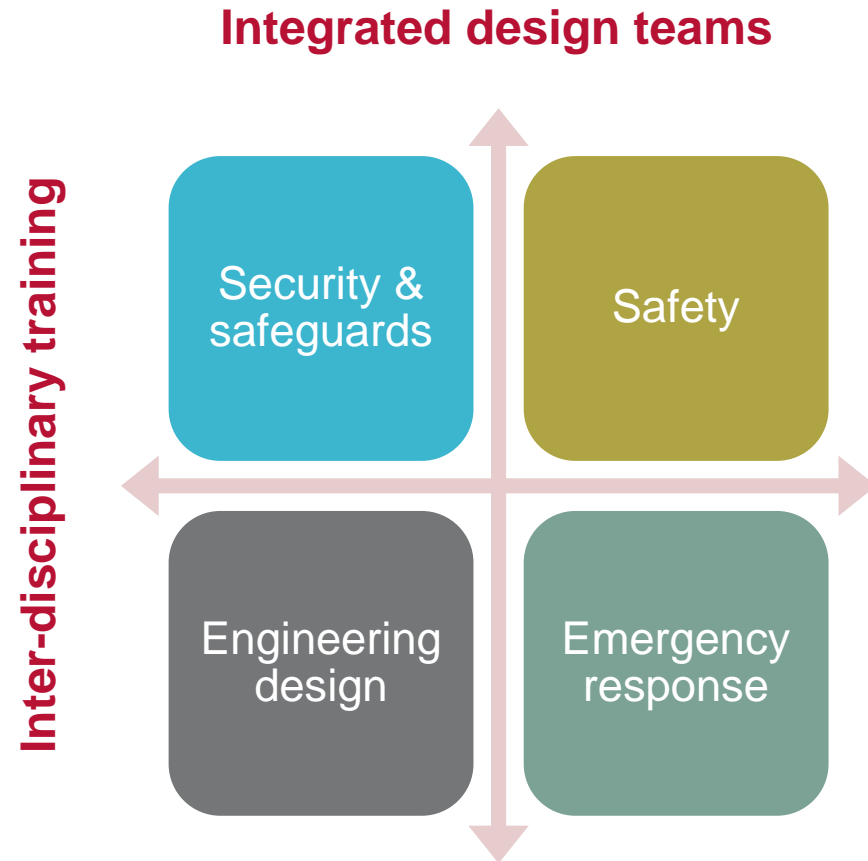
# Design Process



## Stage 0 – Preparation example

- ▶ Examine strategic elimination and substitution options
- ▶ Resourcing
- ▶ Programme governance and assurance for security
- ▶ Security strategy and management plan

# Stage 0 - Resources and training





## Stage 1 - Concept example

- ▶ Develop generic security objectives
- ▶ Develop limited security requirements - intrinsic aspects of the asset design (containment, blast loading, delay etc.)
- ▶ Initial Analysis of facility concept design:
  - ▶ Threat and vulnerability assessment
  - ▶ Freedoms and limitations
  - ▶ Target identification

## Stage 1 – Concept example cont.

- ▶ Identify intrinsic risk reduction options
- ▶ Develop intrinsic risk reduction options
- ▶ Assess the options
- ▶ Refine facility concept design
- ▶ Concept for extrinsic security measures
- ▶ Formulate the security criteria for passing through the main engineering ‘gates’

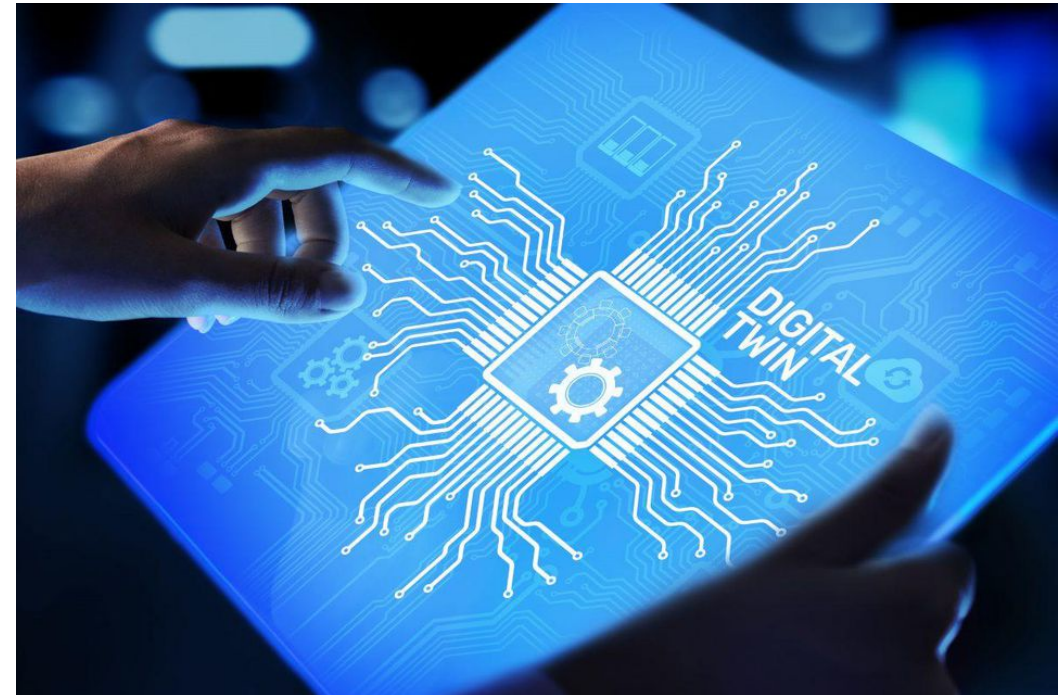
## Challenges in implementing SBD

- ▶ Senior buy-in – Chief Engineer, Programme lead
- ▶ Investment in Preparation Stage
- ▶ Regulatory support to vendors in concept stage
- ▶ Access to host nation Threat Assessment Information
- ▶ Regulatory frameworks – outcome-focused v prescriptive
- ▶ Future-proofing security design



## Determining success in implementing SBD – a few ideas

- ▶ Measure
  - ▶ To what extent security objectives achieved
  - ▶ To what extent intrinsic security requirements met
  - ▶ The value of the intrinsic security design features - computer based software modelling and simulation
  - ▶ The concept design theoretical effectiveness – computer based software modelling and simulation
- ▶ Digital twin concept – there is a digital twin of Singapore, so why not....
- ▶ Concept of ALARP – As Low As Reasonable Practicable





## Summary

- ▶ SBD is:
  - ▶ Influencing asset design to deliver security benefit
  - ▶ Precedes conventional physical and cyber protection system design
  - ▶ New and legacy design
  - ▶ Inter-disciplinary approach based on a defined process and methodology
  - ▶ Significant potential benefits:
    - ▶ Costs
    - ▶ Risk
    - ▶ Resilience



# Questions

E: [a.prior@fnc.co.uk](mailto:a.prior@fnc.co.uk)

M: +44 (0)7896 327033

T: +44 (0)1305 217890