ONR GUIDE			
GUIDANCE ON THE SECURITY ASSESSMENT OF GENERIC NEW NUCLEAR REACTOR DESIGNS			
Document Type:	Nuclear Security Technical Assessment Guide		
Unique Document ID and Revision No:	CNSS-TAST-GD-11.1 Issue 1.2		
Date Issued:	May 2021	**Review Date:**	May 2026
Prepared by:		Principal Inspector	
Approved by:		Professional Lead	
Record Reference:	CM9 Folder 4.4.2.23373. 2021/40575		
Revision commentary:	Issue 1.2 capturing OPEX from GDA process		

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations 2003 (Reference 2). However, for Generic Design Assessments (GDA) the expectation is to produce a Generic Security Report (GSR) that describes a conceptual security regime that will be developed further by a prospective Licensee for a Site Licence Grant application. The licencing process is referred to throughout this TAG but is not described in any detail, which can be found in other ONR documentation.

1.2 The GDA Requesting Party (RP) should take SyAPs into account when developing its GSR throughout the GDA process. The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide but relates exclusively to GDA, which is a voluntary process sitting outside of statutory legislation. The main deliverable in GDA is the GSR. The GSR is a collection of documents that are assessed for the purposes of GDA. The GSR needs to be assessed against SyAPs, which is outcome-focused, thereby offering scope for RP innovation. The GSR is a hierarchy of documents that describe the conceptual security design underpinned by risk-based analysis drawn from Relevant Good Practice (RGP) that might be described as a Security Case and conceptual design requirements.

1.3 After GDA, a prospective Licensee is expected to produce a site-specific Security Plan that is required for licence application and grant then, thereafter, developed for construction through to operation. It is expected that a GSR will form the basis of this plan, as a conceptual design that might be developed next into a detailed design that is site based. Therefore, knowledge transfer from RP to the Licence applicant is an important process towards the concluding stages of GDA. It is important to note that where a prospective new build site is located within 5km of an existing nuclear site, then there is a requirement for there to be an ONR approved civil nuclear construction site security plan to be in place when any work is being carried out, which might be prior to the award of the site licence. Given that there is no nuclear material on the site at this point, a key area of focus for a civil nuclear construction site security plan should be the standards, procedures and arrangements to secure the construction activity (e.g. heavy plant, machinery, power tools) such that it does not affect the security of the adjacent site.

1.4 A GSR, submitted by a RP, based on ONR's guidance, should be developed progressively throughout the GDA process. That process starts with understanding the design of the plant in scope, then identifying and categorising parts of the plant that require protection through a 'graded approach' and then applying 'defence in depth'. Importantly, it should explain the categorisation for both theft and sabotage to determine the applicable physical and cyber protection system security outcomes and postures to be achieved. It is therefore important that inspectors carry out their assessment recognising that the security arrangements detailed in the GSR must be able to meet regulatory expectations so to be of value to a future Licensee. This should be in respect of the relevant security principles so that any future site-specific Security Plan can be developed confidently and ultimately approved. ONR's assessment of the GSR should provide confidence to both the RP and potential Licensee that the conceptual security arrangements for the design in question are considered adequate in that they contain sufficient information, in both scope and detail, to be developed in a timely manner for a license application.

2. PURPOSE, PROCESS AND SCOPE

2.1 This TAG contains guidance to inform ONR inspectors in exercising their regulatory judgment during assessment activities related to the adequacy of generic designs for new nuclear reactors. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed working within the wider GDA process and project management. The GDA Guidance to Requesting Parties (Reference 3) explains the GDA process and ONR's expectations.

2.2 Generic designs may not address some of the site-specific elements which will influence the security infrastructure required at a site and captured in the Security Plan. However, like safety assessments based on a generic site and its characteristics, certain assumptions will need to be made regarding the location of a site perimeter that affects security and especially various Vital Area (VA) identification calculations.

2.3 The Key Security Plan Principles (KSyPPs) are particularly relevant in GDA, although they should be applied selectively and then reflected in the GSR documentation. Of these KSyPPs, 'secure by design' is especially applicable as there is scope within the RP's plant design to reduce security risk at the conceptual stage. The RP might potentially 'design-out' vulnerabilities or reduce consequences in such a way that the security outcome may change. Such an approach could have advantageous resource and cost benefits for the RP although this must be evidence-based. 'Defence in depth' is also a key security principle and the GSR should reflect a concept of several layers and methods of protection. Whilst many of these layers will be determined by the Licensee (particularly personnel and organisational), it is important that the physical and cyber security arrangements, established in GDA, can support the future submissions for Site Licence Grant. Where claims are made on the adequacy of security arrangements, which take into account those measures to be determined by the Licensee, for example perimeter fences, hostile vehicle mitigation etc, there should be a clear statement articulating how the potential Licensee's arrangements are expected to combine with the GSR to mitigate against the threats and consequently meet the relevant SyAPs outcomes.

2.4 This TAG does not prescribe the methodologies for RPs to follow when demonstrating they have addressed the SyAPs and related outcomes. However, there is an expectation that RPs draw from RGP and their submissions are understandable, assessable, timely and of the expected quality. It is the RP's responsibility to determine and describe this detail, reflecting the guidance from ONR to RPs. Then for ONR to assess whether the arrangements are adequate both in scope and detail. This is a joint effort and one of confidence building, ensuring expectations are clearly articulated and managed through the GDA Project's management with regular engagements and progress reporting.

2.5 This TAG focuses on the assessment of generic security arrangements of the RP's design and does not deal with the administrative security arrangements for handling Sensitive Nuclear Information (SNI) or workforce trustworthiness. The RP must comply with relevant UK legislation to ensure the protection of information. Access to the UK's Design Basis Threat is critical to completing GDA. Clearly before embarking on GDA, the RP should engage with ONR to ensure the arrangements for managing and exchanging SNI is in place.

3. RELATIONSHIP TO RELEVANT LEGISLATION

3.1 The GDA process sits outside the formal ONR regulatory regime and vires. It is, therefore, undertaken on a voluntary basis by the RP, through the appropriate UK

Government department. It is conducted through a contractual arrangement with ONR to allow for cost recovery.

4. RELATIONSHIP TO IAEA DOCUMENTATION AND OTHER GUIDANCE

4.1 There is an expectation within GDA that the RP draws from RGP. While ONR operates a mainly non-prescriptive regulatory regime, the RP should underpin their evidence with credible and targeted RGP of international and UK origin.

4.2 The International Atomic Energy Agency (IAEA) document 'Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities' Nuclear Security Series (NSS) No 13 (INFCIRC225 Revision 5) (Reference 4) contains principles and recommendations the UK is obligated to consider.

4.3 The IAEA Technical Guidance Document 16 'Identification of Vital Areas at Nuclear Facilities' (Reference 5) and 4 'Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage' (Reference 6) provide further related guidance.

4.4 This TAG is consistent with the principles described in the international and national documents highlighted below.

4.5 The IAEA document INFCIRC225 Revision 5 at paragraphs 3.45 to 3.47, supporting Fundamental Principle I: 'defence in depth', details that physical security arrangements require a mixture of hardware, procedures and facility design. It also states that the physical protection functions of detection, delay and response should each have 'defence in depth' and use a 'graded approach' (Fundamental Principle H) to provide appropriate effective protection against insiders and external threats (Fundamental Principle G).

4.6 The IAEA technical guidance document 'Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage' at section 3.5.1 reviews what constitutes a physical protection system and at section 3.5.2 discusses the need for Vital Area Identification (VAI).

4.7 Within the NSS documents there are other relevant publications together with useful guides produced by the World Institute for Nuclear Security. Increasingly, academia and Centre for the Protection of National Infrastructure (CPNI), together with the National Cyber Security Centre (NCSC), will provide documents that assist a RP and identify relevant standards. Security-based professional organisations also provide a source of thinking on 'secure by design'. ONR would encourage any RP to widen its source of guidance to inform its thinking and embrace innovation intelligently when taking a risk and evidence-based approach to their design.

4.8 As part of choosing RGP, the RP is also encouraged to draw from operational experience from current power plants and elsewhere although this should not be used without arguments and evidence. Moreover, inspectors' assessments should be informed by earlier GDAs, learning from previous RP submissions and ONR reports. Inspectors should seek access to any Knowledge Management sources that would inform the process and guide subsequent judgements particularly before GDA is commenced as part of individual inspectors' preparation.

5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS

5.1 The HMG publication Government Functional Standard GovS 007: Security (hereafter termed GovS 007) (Reference 9) describes expectations for security risk management, planning and response activities for cyber, physical, personnel, technical and incident management. It applies, whether these activities are carried out by, or impact, the

operation of government departments, their arm's length bodies or their contracted third parties. The security principles, governance, life cycle and practices detailed within GovS 007 have been incorporated within SyAPs. This ensures that all NISR dutyholders are presented with a coherent and consistent set of regulatory expectations for protective security whether they are related to government or not. As an RP will be handling SNI directly, and through any contractor, these expectations are relevant and require early consideration.

5.2 The Government Security Classifications document, together with the ONR Classification Policy (Reference 10) describe types of information that contain SNI, the level of security classification that should be applied, and the protective measures that should be implemented throughout its control and carriage.

5.3 The UK Government's DBT document (Reference 9) refers to the malicious capabilities that are required to underpin the Vital Area Identification (VAI) process. It is also used in the design and evaluation of physical protection systems against relevant SyAPs security outcomes once the site has been fully categorised for theft and sabotage. The RP may choose to develop a form of threat identification document that draws accurately from the DBT and associated Cyber Security RGP relating to the threat. A foreign RP would be expected to use a UK based contractor with the right clearances so to apply the DBT.

6. ADVICE TO INSPECTORS

6.1 Before a GDA starts, the ONR lead security inspector should ensure there is an in-house team with dedicated Safety Informed Nuclear Security (SINS) and Cyber Security and Information Assurance (CS&IA) expertise. That team should ideally have GDA experience to ensure there is continuity of assessment methodology. The Security team should draw on any learning from previous GDAs. They should first develop a good working knowledge of the proposed RP's design and any security features already inherent in the design. If the RP has a relatively mature design, that already incorporates some security systems, structures or components, then an early joint activity with the RP will be to understand the gap between its design and ONR's expectations under a SyAPs based approach. The fact that designs from outside the UK may meet other regulator's expectations does not necessarily mean it will be adequate against UK's regulatory framework. This might be because of different approaches being used and/or because the DBT or other elements of government risk appetite differ from that of the HMG. Therefore, assessments undertaken in other county's regimes will need to be discussed within the wider ONR GDA project team in terms of their value.

6.2 Within GDA, and to avoid any 'stove-piping', the security team must work within the ONR project team. The format and arrangements for carrying out a GDA are defined by ONR (Reference 3) and actioned through the project's management team. As GDA is a stepped process, the security inspector is required to provide an Assessment Plan for each step and, at the close of that period, produce an Assessment Report. The wider security team, including CS&IA and SINS expertise, contribute to the report. For audit purposes, specific security-based reports from various experts may underpin the project-based security assessment report at each step.

6.3 Experience suggests GDA requires significantly more cross-specialism cooperation than in other areas of regulation. This requirement is explained within ONR's guidance and is expected to be outlined in any assessment plan for various steps within GDA. The RP's security risk analysis draws from the safety case and any modifications to the design will inevitably be managed through an integrated process. Consequently, it is important that the security assessment is integrated into the wider ONR and

Environment Agency (EA) assessment process so to manage any potentially conflicting requirements. For example, in assessing cyber security risk and related controls, security inspectors will work jointly with other related specialisms. Similarly, security inspectors should verify, through their RP counterparts, any design changes arising for safety and/or environmental reasons having taken due account of potential impacts on security. It is expected that the RP's security team is embedded in any modification process, that is an essential part of applying a 'secure by design' approach.

6.4 With the adoption of SyAPs, the RP's agreed submissions, comprising of the GSR and supporting documents, would need to provide adequate and meaningful claims, arguments and evidence to underpin such arrangements that are best described as their security regime concept. The RP is free to describe the GSR structure and subordinate documents that address risks, outline methodologies used and report the result of their analysis that underpins the security concept. These overall conceptual arrangements would form the basis of the future approved security plan. The process of licencing and early construction is explained in the Construction Site TAG TAST-GD 6.6 (Reference 10) and is part of the potential licensee's case for site licence grant.

6.5 ONR security inspectors should ensure that the GSR submission from the RP clearly defines the scope of the plant covered. Should the technology described in the GSR be subsequently deployed in the UK, the assessment of the complete design at the site, possibly as a multi-unit installation, will be focused initially on those areas not assessed as a part of the GDA scope. However, the licensee should build on the GSR, therefore there needs to be an effective method of transferring knowledge from the RP to the licensee.

6.6 Because GDA is a phased process, it encourages the RP to develop, progressively, what might be described as a security case that justifies a conceptual security design. Such language and frameworks are described within SyAPs. Whilst being non-prescriptive, SyAPs offers a common lexicon and draws from RGP. ONR security inspectors are required to advise, then make judgements, in developing their response to the RP's submissions. Initially, in understanding a SyAPs based approach, the security inspector should ensure that the RP has identified all relevant Fundamental Security Principles (FSyPs), with Security Development Principles (SyDPs), and drawn from the KSyPPs. Thereafter, through the early steps of GDA, ONR would seek assurance that the RP has carried out a risk assessment process that would inform their security concept and meet the expectations within the relevant aspect of SyAPs with its outcome-focused approach. Regular engagement with the RP throughout the GDA process is essential to fully understand their proposals and influence the quality and completeness of their early through to final submissions. ONR will influence and advise the RP as documentation is refined and matures so to meet the expectations at the end of the final step of the process, allowing enough time for concluding assessments and governance to take place.

6.7 Looking at specific aspects of GDA, and early in the process, ONR will wish to assess the RP's methodology for identifying and categorising risks that have security consequences. This would enable the RP to take a 'graded approach' and is the starting point for any measures to achieve 'secure by design'. Methodologies are not prescribed, but RGP is expected to be used to assess risks posed from cyber, insider and physical attack or a blend of these vectors. The security assessment should therefore cover target identification, and this requires detailed knowledge of the safety case. The UK DBT must be used in the design and evaluation of a prospective site's protective security system to provide assurance that it achieves the appropriate SyAPs outcomes and therefore aligns with government risk appetite.

6.8 Ultimately, ONR security inspectors should consider whether the RP's submission demonstrates that the proposed generic security measures will meet the appropriate SyAPs outcomes. Part of meeting this expectation is a regime that achieves adequate 'defence in depth'. In achieving this outcome, it maybe that a security design concept includes aspects of the wider site or makes claims against broader site-based protection. Even if the wider site is not in GDA scope, taking credit for future site-based security arrangements is acceptable in GDA. That is to achieve a specified outcome, there is a commitment that the licensee will adopt such additional measures having taken a conservative approach to risk. If such claims are going to be made in GDA, then they need to be raised early in the process with ONR.

6.9 Working within the wider ONR project team, and towards the end of GDA, judgements will be made regarding any deficiencies in the final submissions or aspects that need further definition or modification at the close of the GDA process. Most likely these should be recorded as residual matters and designated 'assessment findings'. Where these are substantial in scope, quantity or importance they should be recorded as more significant issues. However, it is expected that within the development of the GSR, any real GDA 'issues' would have been identified in previous steps. The methodology to record these findings is found in ONR's GDA guidance and supporting documents together with instructions from the project management team. Depending on the maturity and scope of the RP's design, and within the security conceptual design, certain detailed choices on the exact specification of security infrastructure technology would normally be left to the licensee. Achieving the right balance of GDA requirements and those for the licensee to decide is essential to any GDA judgement and is different for each specialism. Balanced judgement is part of early GDA deliberations and requires mutual agreement between ONR and the RP for a GSR to be considered 'meaningful'. The RP will have arrangements to ensure that any commitments made in GDA are transferred efficiently to the licensee as part of knowledge transfer.

7. GENERIC SECURITY REPORT DEVELOPMENT

7.1 The output expected from the RP at the end of GDA is the GSR. Like the RP's safety case, the GSR is best described as a security case and conceptual arrangements that would feed into a site-specific security plan. The GSR should be adequately underpinned by evidence that demonstrates either that RGP or an equivalent standard has been achieved. Therefore a 'claims-arguments-evidence' approach, inherent in SyAPs, is encouraged so to be aligned with safety. Also, in a similar way to safety, the GSR should be principle and risk based together with outcome-focused (or 'goal setting').

7.2 Based on safety case experience and security RGP, and in terms of structure and a working framework, the GSR may be a series of tiered documents with a header document as a summary. This header or 'capstone' document might be read 'standalone' and a version made widely available on public-facing websites. Under the 'capstone' document there maybe second and third tier documents that explain the methodologies used together with the output from that analysis by way of the conceptual security regime. Therefore, the GSR, as a set of documents described within a framework of submissions, and updated through any design change, is developed incrementally throughout the GDA timeline.

7.3 Developing the GSR is therefore a process with building blocks. First methodologies for assessing risk (usually to identify and categorise Vital Areas and a Cyber Security Risk Assessment and report) are explained and agreed. Thereafter, these methodologies are applied to the design as it is modified for UK use. The RP's framework for applying 'secure by design' could then be described within a supporting

document given the importance of KSyPP 1 (Secure by Design) to the GDA process. The GSR, developed by the RP, will have several key features as described later in Section 8. The GSR must identify the targets requiring protection and the features built into the plant to provide protection to those critical assets and related areas. Any concept should reflect the 'defence in depth' principle and be described in enough detail to enable a future licensee to turn the GSR into a security plan. This level of detail would expect to include a consideration of security categorisation and classification at KSyPP 5 and any relevant codes and standards applied at KSyPP 6.

7.4 Not all GDAs will be the same in terms of the detail developed by the RP for licencing and construction. The detail available at the time the GSR is submitted will be dependent on the maturity of the reactor design and chosen buildings in scope. The scope of GDA will be agreed with the RP early in the process and those areas to be assessed and sampled clearly defined by ONR. This will be ONR project driven and not exclusively about security. However, in all GDAs there should be clear statements regarding those aspects of security that will be developed, after the GDA process, by the prospective licensee. The interface between RP and future licensee is a key feature for engagement during the latter steps of GDA.

7.5 Early engagement with a prospective RP is of benefit in achieving an initial mutual understanding of ONR's GDA expectations. While this is outside the GDA formal process, it is important that the inspector can gauge the level of the potential RP's understanding of ONR's expectations and design maturity especially if security features are already built in. Once in GDA, this mutual awareness can be further reinforced by the early submission of an introductory security report, usually part of the preliminary safety and security report, which demonstrates the level of RP knowledge and capability to deliver a meaningful GDA. In taking an innovative and flexible approach, the RP may present an existing security plan of a similar design on another site to help articulate their understanding and provide the security inspector with a means to start engagement and assessment. GDA is not an inflexible process and, through early engagement, any innovative approach selected by the RP might be examined in detail so there is mutual understanding and agreement on how to progress with delivering a security case and conceptual arrangements.

8. KEY ELEMENTS OF A GENERIC SECURITY REPORT SUBMISSION

TARGET IDENTIFICATION

8.1 Target identification should be carried out at an early stage of the GDA process to ensure there is enough time to consider the potential to design-out vulnerabilities or build-in the necessary security arrangements to mitigate the threat. Targets will include Nuclear Material and Other Radioactive Material (NM/ORM), any associated operational technology and some other specific Structures, Systems and Components (SSCs) related to fundamental safety functions. Therefore, as a starting position, the RP needs to establish the nuclear inventory and then, drawing from the safety case, those protective and mitigating safety SSCs. Together with an understanding of the design in detail, the RP can then identify what to protect, its location, its relative importance and attractiveness so to shape a security protective concept.

CATEGORISATION FOR THEFT AND SABOTAGE

8.2 Before the RP's Security team starts its analysis of targets and the application of 'secure by design', they need to be clear on the buildings in scope described through existing design and plant information documentation. That information should identify the nuclear inventory together with fundamental safety functions (and any subordinate high-level safety functions) with a general layout that includes properties of civil

structures, modes of operation and means to control the plant's operations and emergency plans for escape. A 3D model or similar graphics would aid early engagement between the RP and ONR's security team so to set the scene for categorisation for theft and sabotage.

8.3 The RP should have an appropriate process in place to identify theft targets through categorisation of its NM/ORM inventory. Guidance on identification of theft targets and categorisation can be found in TAG Target Identification for Theft CNS-TAST-GD-6.1 http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.1.pdf

8.4 The GSR should identify Vital Areas, consistent with the UK definition, by using the UK DBT (Reference 9) which is mandatory and drawing on other threat-based information including the latest RGP guidance on the Cyber Security threat. Guidance on the identification of vital areas is contained within TAG Target Identification for Sabotage – CNS-TAST-GD-6.2. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.2.pdf

8.5 The categorisation of NM/ORM and facilities for both sabotage and theft is essential as this will determine the initial security outcomes to be achieved. Then, through 'secure by design', the RP can potentially reduce the security outcome by lowering inventories or reducing radiological consequences by modifying the design to passively mitigate vulnerabilities to the DBT (e.g. by increasing robustness, resilience, redundancy or segregation). The various categories of Vital Area, and their thresholds, are detailed in the SyAPs OFFICIAL-SENSITIVE: SNI Annexes. These thresholds are based on the UK Government's risk appetite related to radiological consequence that could potentially affect the public.

8.6 The benefit of taking a 'secure by design' approach is that analysis of the nuclear inventory and vulnerabilities within safety systems to malicious attack all inform the level of risk. As stated above, that risk maybe reduced through specific design modifications that decrease, or even eliminate any dose consequence to the public resulting from a worst case DBT attack. That analysis could then be used as evidence to shape the security regime accordingly. This might have benefit to the RP from a commercial perspective by simultaneously increasing the protective security system effectiveness and efficiency. Security inspectors should be aware of these wider considerations.

8.7 Characterisation of the design, and the categorisation for sabotage and theft, is the essential part of the early stages of GDA and requires agreed methodologies for analysing all forms of security risk through applying the UK DBT. To complete this work requires expertise in VAI and NM Categorisation, Cyber Security Risk Assessments and developing a conceptual security regime. Should the RP wish to achieve a high tempo in meeting GDA expectations, then such expertise would be considered as indispensable. Inspectors would expect the RP to either have such expertise 'in house' or use the supply chain for suitable nuclear safety and engineering knowledge. Establishing an effective SQEP capability early in GDA is judged as essential.

8.8 More information on VAI and NM Categorisation is provided by specialist inspectors.

CYBER SECURITY

8.9 Within the scope of the GDA, the RP must demonstrate how the cyber protection system outcomes will be met. This should be in detail for the main safety control systems. For the computerised security systems, a more proportionate 'due diligence' approach is required so to demonstrate that there is sufficient power, back-up power, room and space, in-built security and ventilation systems to support a reasonably

foreseeable security system so to inform a design concept of operations detailed in the GSR series of documents.

8.10 As part of the Security team, the CS&IA inspector will be expected to gain the good understanding of instrumentation and control and plant systems working with other ONR inspectors (mainly Control and Instrumentation (C&I) specialism). Of specific interest will be the types of Computer Based Systems Important to Safety (CBSIS) and other related systems, their functions and location together with any controls already planned for the conceptual design. There will be a cyber element to the DBT analysis, and the RP may also supplement that with information from public sources and RGP. Like all RGP, the sources of such advice should be discussed with the CS&IA inspector in terms of its credibility.

8.11 The GSR should provide details of the methodology for the assessment of risk of cyber intrusion and malicious action against centralised instrumentation and control systems associated with SSCs within the design that could result in an Unacceptable Radiological Consequence (URC) and hence become a vital area. Such control sets would aim to prevent or mitigate the effects of a cyber-attack and include consideration of the 'insider threat'. The GSR should define the threats to these CBSIS as part of Operational Technology (OT) and Information Technology (IT) including software. The RP is required to assess the level of cyber security risk against these systems and then seek potential security-based design improvements by applying a 'secure by design' approach. Where a control is considered a future licensee issue, ONR would wish to see the related enabling activities considered during GDA.

8.12 Whilst the focus may be on the risk assessment of individual CBSIS, the overall architecture of the plant should also be considered to support 'defence in depth'. Consideration should also be given at the component level so to demonstrate 'production excellence' for cyber security.

8.13 Guidance on the identification and categorisation of operational technology can be found in TAG Protection of Nuclear Technology and Operations -TAST-GD 7.3. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-7.3.pdf

8.14 It is important that OT and IT risks are identified and effectively managed. A fundamental aspect of this is categorisation in line with the tables in the SyAPs annexes. Identification and categorisation of OT and IT should allow the RP to design an effective cyber protection system using a graded approach to achieve the relevant cyber security outcome. Further guidance for inspectors can be found in the TAG Effective Cyber and Information Risk Management - TAST-GD-7.1. http://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-7.1.pdf

8.15 As part of delivering a meaningful GSR, the RP is required to provide a cyber security risk assessment report underpinned by an agreed methodology. That report should feed into the identification of vital areas and identify security control sets that will be part of the description of the RP's conceptual security regime. There is also a requirement to identify CBSIS that needs protection albeit when a malicious intrusion would not necessarily lead to a URC, if compromised. The division of assessment and reporting between the CS&IA inspector and C&I inspector should be made clear to the RP early in GDA. However, there needs to be a close joint approach both internally and within the RP's related teams.

9. GDA SUBMISSION REVIEW PROCESS

9.1 GDA is a process, usually involving several steps, that is progressive and considered within ONR's regulatory guidance of which security is just one part. There are over fifteen safety technical disciplines within GDA assessments and similar assessments

from the EA. ONR's various guides on GDA explain the expectations in terms of the RP's safety case and security equivalent represented by the GSR. The logic behind a stepped process is that the RP has time to develop and refine their major submissions with ONR taking an enabling approach throughout. That approach involves assisting the RP to deliver a meaningful GSR that will in turn inform any potential licensee in meeting regulatory expectations for granting a licence. Unlike other aspects of ONR regulatory activity, the RP is not under our regulation less those specific aspects of NISR that relate to SNI. Security inspectors, forming a dedicated team, and working closely with safety colleagues, will agree an engagement programme with their equivalents in the RP's organisation. This will be carried out with ONR providing advice at formal meetings and assessing the submissions for adequacy reflecting ONR's GDA guidance. The security inspector should ensure regulatory expectations are clearly stated and understood by the RP working with a specified meeting protocol. Consequently, at the start of a given step in GDA, the arrangements will be captured in an Assessment Plan. It is only at the end of each step that a formal report must be produced, and these maybe published on ONR's website. As GDA in the future will be flexible, the reporting regime may change.

9.2 The expectation in GDA is that the RP will have a SQEP security team that can manage modifications and extract from the safety case to inform security-based risk assessments that feed into the GSR. ONR, equally, requires a similar capability to assess the RP's submissions. ONR security inspectors should therefore become familiar with the general reactor technology and, specifically, the design under GDA acknowledging its level of maturity and whether it has already been subject to other regulatory scrutiny. The RP should confirm the status of the design's maturity, what security features exist and underlying justification, describe what RGP they will use (maybe have already used) and any learning from existing operating plants especially of similar design. Thereafter, it is important to understand the RP's approach to delivering a GSR and specifically the methodologies to be used to analyse risk whether from physical, insider and cyber means but informed by the UK DBT (the RP must have ready access to the DBT).

9.3 ONR security inspectors will be working within the wider GDA project and steered by guidance to RPs and related GDA Technical Guidance (Reference 11). In general terms, ONR security inspectors should discuss the GSR format with the RP at the start of GDA. This should include the scope and level of detail in the GSR that would be considered as meaningful as described within ONR guidance. For example, the GSR security regime concept should provide sufficiently detailed security requirements, drawing from KSyPP 5, in such a way that the future licensee would be able to develop these further into functional and technical requirements. This line of thinking is dependent on the maturity of the design and ONR will acknowledge this during its assessments. In the early steps of GDA, ONR will review the outline of the RP's GSR submission and strategy to develop it. It is accepted that the GSR itself, as a document, would not include all analysis that contributed to any claims, arguments and evidence. In GDA what is submitted for assessment, and other supporting analysis, should be agreed early in the process. Also, as a matter of a regulatory approach, ONR would not necessarily assess all this material but will target through sampling.

9.4 An illustration of what might be included in the GSR is described in Appendix A. Security inspectors would expect the GSR document set to include both methodologies used and a description of the conceptual security regime. RGP would be used throughout. For example, documentation should identify the various security functions (delay, detect, assess etc) to be delivered to meet the relevant SyAPs outcomes. The claim that an outcome is met should be supported by appropriate arguments and evidence to justify a specific security function will be achieved to a defined posture. However, the exact ways and means the RP describes these

requirements is not prescriptive and focus should always be on achieving the SyAPs outcome rather than the indicative postures.

9.5 It is anticipated that the GSR will include several layout drawings as supporting evidence together with other diagrams that provide a suitable pictorial narrative. The RP should verify that all the latest information has been included in the submission. Inspectors should be mindful that the RP's change control process will be vital in ensuring the most up-to-date designs are being assessed.

9.6 Throughout the GDA process the design will develop, partly as a result of interactions with the regulators, and new information will be received. It is likely, therefore, that several GSR document set iterations will be received, usually based on 'design reference points'. As the design is modified at each reference point, the documents that underpin that design will be 'frozen' to control the assessment process. The management of various key submissions over time, against such design references, is the responsibility of the GDA Project Management Team. Following regular security joint RP/ONR meetings (at Level 4), it is expected that the RP would maintain an audit trail that evidences ONR's responses and expectations throughout the GDA process. This process aims to manage ONR's actions placed on the RP, modifications to the design and any commitments for the licensee to honour. ONR security inspectors should have similar controls in place usually by recording meetings through a Contact Record and captured through the project management team. If necessary, and within the wider GDA process, regulatory queries and observations maybe used as a tool to seek improvement in the RP's submissions.

10. FINAL GSR SUBMISSION

10.1 The final iteration of the GSR document 'set' forms part of the RP's submission for end of GDA assessment. It will be assessed by ONR security inspectors taking account of all relevant FSyPs and SyDPs and related TAGs. The security team's assessment report will assist with compilation of the project assessment report at the end of the GDA process. However, as GDA is progressive and ONR are enabling, the final submissions will have been developed over the various steps so that the closing GDA assessment should not present any surprises. Essentially, inspectors should verify that the relevant outcomes have been identified and that adequate arguments and evidence to support the achievement of those outcomes have been provided by the RP. At the end of the final ONR assessment period, the security team's assessment report will draw from previous step reports and be informed by both CS&IA and SINS assessments. These specialist assessments and reports would ensure there is a robust audit trail and would also contribute to security knowledge management.

11. REPORT PUBLICATION

11.1 The format for the GDA assessment reports will be provided to ONR security inspectors by the GDA project management team. The intention is that all technical assessment reports will be published on the ONR website. Therefore, the ONR security inspector should write a report that does not contain SNI but still offers as much detail as is reasonable so to be transparent and informative. ONR security inspectors should consider annexing SNI or producing supporting reports at a higher classification where it is considered beneficial to expand on the reasons for judgements being made - hence for any audit - and the content would warrant the higher classification. So, any SINS and CS&IA internal supporting reports, that feed the main security assessment report, could be at a higher classification and would not be published. Any SNI based annex or separate report should not be published on the ONR website but should all the same be shared with RPs.

12. REFERENCES

1. ONR Security Assessment Principles.

2. Nuclear Industries Security Regulations (NISR) 2003 (as amended) Statutory Instrument 2003 no.403.

3. ONR Generic Design Assessment Guidance to Requesting Parties.

4. IAEA Nuclear Security Series No.13 – Nuclear Security Recommendations on the Physical Protection of Nuclear material and Nuclear Facilities (INFCIRC/225/Revision 5) January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

5. IAEA Nuclear Security Technical Guidance Document No.16 – Identification of Vital Areas at Nuclear Facilities http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf

6. IAEA Technical Guidance Document Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage www-pub.iaea.org/MTCD/Publications/PDF/Pub1271_web.pdf

7. Government Functional Standard 007. Cabinet Office.

8. Classification Policy for the Civil Nuclear Industry. ONR.

9. UK Design Based Threat.

10. Nuclear Construction Site TAG (CNS-TAST-GD-6.6).

11. New Nuclear Power Plants: GDA Technical Guidance GD-007 Revision 2 Nov 19.

12. ONR Safety Assessment Principles.

13. GLOSSARY AND ABBREVIATIONS

ALARP	As Low as Reasonably Practicable
BPC&I	Basic Process Control & Instrumentation
CBSIS	Computer Based Systems Important to Safety
CBSy	Computer Based Security Systems
C&I	Control and Instrumentation
GSR	Generic Security Report
IAEA	International Atomic Energy Agency
IT	Information Technology
NCSC	National Cyber Security Centre
NIMCA	Nuclear Industries Malicious Capabilities (Planning) Assumptions
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NMAC	Nuclear Material Accountancy & Control
NSSP	Nuclear Site Security Plan
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
OT	Operational Technology
SAPs	Safety Assessment Principles
SINS	Security Informed Nuclear Safety
SNI	Sensitive Nuclear Information
SSCs	Structures, Systems, Components
SSP	Site Security Plan
SyAPs	Security Assessment Principles
TAG	Technical Assessment Guide
UPS	Uninterruptable Power Supply
VA	Vital Area
VAI	Vital Area Identification

APPENDIX A

THE GSR – A POSSIBLE FORMAT, CONSIDERATIONS AND ASSESSMENTS

1. The purpose of this additional guidance is to provide further context to the Security GDA TAG. It is not intended to be exhaustive but may assist security inspectors when judging the adequacy of the RP's case. It draws from experience in assessing recent GDAs.

2. Whatever the design entering GDA, there is always scope for any RP to apply a 'secure by design' approach. An RP may have already designed-in security drawing on the benefits inherent in that design's safety features. On these occasions, the inspector would wish to identify any gap between the RP's security analysis that justifies their design and ONR's expectations. Also, it is possible that a foreign design may not have the security features that would meet ONR's expectations due to differences in respective countries' DBTs or government risk appetites. Whatever the RP offers as the design on entry to GDA, any security claims would need to be substantiated using RGP methodology and meet SyAPs based expectations reflecting an 'outcome' based approach.

FORMAT

3. A possible GSR format could be a tiered approach. At the top might be an 'header' document, that is the published GSR. That document could provide an overview of the selected GDA approach, key methodologies chosen, their product and how that justifies the conceptual security regime. Within the document it could include how the RP has adopted a SyAPs based approach albeit selectively as some aspects of the document are more relevant to GDA. It should explain how the RP intends to provide evidence of meeting the outcomes specified within SyAPs. A header document could be sufficiently meaningful when read in isolation. It should also provide a suitable entry point for the subsequent subordinate submissions that would provide the evidence to support security claims by the RP as meeting ONR's expectations.

4. To provide a logical sequence to the RP's submissions, subsequent tiers (for example Tiers 2-3) after the GSR header document or Security Case, could include methodologies used, threat-based analysis, a VAI report, a cyber security risk assessment report and a description of the conceptual security regime. This is not an end in itself but should aim to inform a potential licensee's development of the GSR towards a security plan that is also SyAPs aligned. Further tiers, that might offer deeper analysis that provide further evidence to support the GSR, could be submitted to ONR or used to inform the potential licensee. Within these documents it should be clear what topics would be for a future licensee to consider. The future licensee would not only need the requirements of a conceptual design but also its justification based on analysis of the plant design and inherent security risks with specific calculations as they relate to the extent of the risk in terms of radiological consequences of sabotage.

5. The GSR should sit within, and alongside, other key GDA submissions and might be collated into a report that covers safety, security and environment. Within GDA, there is a need to coordinate and, if desired, de-conflict security requirements with others to enable the safe and effective running of the plant. Within the GDA process, the RP must understand this need and demonstrate such de-confliction has been considered and its implications managed

satisfactorily. ONR would seek evidence. For example, the RP's modifications procedure that enables such collaboration between specialisms.

6. The RP might, at the start of GDA, explain its strategies for producing and then developing the safety, security and environmental cases. That document might explain how the GSR would be developed over the GDA period. It could explain the objectives and scope of the documents to be submitted. Also, the hierarchy of submissions that could explain their claims, arguments and evidence, if chosen as a framework. It could describe the level of detail GDA will offer in the security domain to enable a future licensee to develop security requirements. It might list RGP used to justify their conceptual design, the organisation needed to deliver the documents and their SQEP together with internal assurance arrangements. This list is not exhaustive and early engagement with ONR would set the foundations for any GDA.

REFERENCE DESIGN

7. The Reference Design for GDA is explained within ONR guidance. Any external design will need to be adapted for UK purposes by meeting ONR's expectations. In contrast with other states, the UK operates under a different regulatory scheme based on SyAPs and one that is mainly non-prescriptive. The Reference Design's features, as they may add security value, might not in themselves meet UK expectations based on an outcome-focused regulatory philosophy. Therefore, the RP will need to demonstrate how they meet UK expectations in terms of the DBT, risk analysis including VAI and NM categorisation and the outcomes and principles inherent in relevant parts of SyAPs. It should be noted that in security assessments and judgements, ALARP is not used as a framework to establish acceptable residual risk. Instead, the RP must use RGP in their arguments and evidence to demonstrate they have met the specified outcomes and relevant principles in SyAPs in controlling risk. This is known as the 'graded approach' and can be considered to be broadly equivalent to demonstrating that risks have been reduced ALARP.

8. Should the proposed design be UK-based, and the RP already aware of ONR's expectations, together with some of these inherent in their design, then the approach by ONR will need to be tailored accordingly. Security inspectors should be prepared to be flexible and understand the RP's starting position and ambition for achieving a Design Acceptance Certificate or, if not, a GDA statement. Ideally, a UK RP planning for a shorter GDA should have a SQEP team in place at the start of the process having held confidence-building pre-GDA meetings with ONR. These pre-GDA meetings could allow the prospective RP to fully appreciate what ONR expects by way of substantiated claims together with the basis for assessment (for Safety it is ALARP, EA use Best Available Techniques and for Security it is SyAPs and specified outcomes in line with the graded approach).

SECURITY 'GOLDEN THREAD'

9. The idea of a 'golden thread' is raised in the guide to RPs. Within the GSR header, and Tier 2 documents, the RP should describe the 'golden thread'. That thread of claims and evidence should 'tell the story' from applying SyAPs principles through to the description of a conceptual design for security in sufficient detail to enable the potential licensee to develop that GSR document set into a security plan thereby meeting relevant legal requirements. That thread might be summarised as follows:

- ONR expectations are described in SyAPs (selected parts include KSyPPs, FSyPs 6 (Physical Protection Systems) and 7 (CS&IA) and 'outcomes' and 'postures'). Also, in the various TAGs intended for their guidance (GD 11.1 and 6.2 included). Safety TAGs may also inform judgements including those relating to electrical power and more generally on the safety case.

- ONR guidance draws from IAEA documents including INFCIRC/225/Rev5 and related guides for vital areas and insider threats. These are RGP.

- Considering SyAPs and such guides, the RP should describe the methodologies they have selected to identify and categorise security risks. As a perquisite, the RP needs to understand the plant, its structure and operations. Importantly, to know the nuclear inventory, hence radiological risk, and critical safety systems.

- The RP should, through understanding their plant design, be able to explain the inherent security already within the features of that design. This might be a starting point as improvements in passive safety, stronger containment, simplified systems, reduced inventories together with reduced waste may, if sufficiently argued, reduce the radiological risk. Conversely new fuels and remote control could increase certain risks. Whatever these new features are that may reduce risk, they will need to be substantiated.

- To understand risk, the RP needs access to the safety case. Drawing on the safety case, the RP should establish what to protect, why in terms of consequence and therefore relative importance of systems, processes and areas (e.g. considering any vital areas and whether they are subject to 'direct and 'in combination' malicious events). To identify their locations and include considerations of identification and exploitability of any vulnerability as they relate to these critical assets in terms of a malicious act. Usually these would include the areas with nuclear inventory, safety SSCs, CBSIS and the fuel route.

- Understanding how a threat scenario - a blend of physical, cyber and insider elements - based on the UK DBT might initiate an event that leads to theft and/or a URC.

- Investigate where inherent safety functions, and the structure of the plant, could reduce the security risk or where further engineering might do so through selective modifications. That is design-out vulnerabilities or reduce them and hence the radiological consequences of a malicious event.

- If 'secure by design' cannot be achieved through modifying the design, and risks not reduced, then what is the consequential 'outcome' (in SyAPs' annexes) required and hence related level of mitigation sought? The RP should, once the level of risk is known (including vital areas), proceed to design-in a security conceptual regime that would then achieve the desired outcomes. With a non-prescriptive regulatory approach, that mitigation that meets the specified outcomes in SyAPs should draw on RGP and be evidence-based.

- The RP should ensure that security arrangements and features do not hinder safety and the operation of the plant especially under emergency conditions. Consequently, cross-function coordination needs to take place to ensure de-confliction of any incompatible

requirements. Security outcomes must, nonetheless, be realised but there is flexibility in how this is achieved within GDA or alternatively by the licensee.

- In describing the security regime, with its features and arrangements, the RP should draw from RGP. Therefore, security functions e.g. detect, delay, assess, respond, mitigate and others like deflect, disperse, disguise and stand-off and for Cyber to identify, defend, detect, respond and recover, are used to meet specified security principles (e.g. 'defence in depth', zoning/security areas and a 'graded approach').

- The RP is then expected to describe the security functions that deliver the desired effect. Functions might be described in more detail in several ways. Capability, for example, might be divided into people, processes and equipment. In some GDAs the RP may be able to describe capabilities in detail, while in others they may simply describe a methodology for achieving depth and a graded approach. That methodology might identify security functions and their classification as they relate to parts of the plant design (KSyPP 5.1 and 5.2 (Cat & Class)) so to target risk and deliver comparable mitigation. The licensee would adopt that methodology to underpin their more detailed security requirements and maintain the 'golden thread' from GDA.

- With more mature designs entering GDA, the RP may be able to describe the security regime in greater depth and granularity. In that way, various security capabilities might include descriptions of access management, searching, command and control, power, control of the workforce (e.g. 2-person rule), ways to enabling plant operations and emergency access. These might then be divided into systems, structures and arrangements such as access control points, lighting, Automatic Access Control Systems, Close Circuit TV, Intruder Detection Systems, power, cyber controls, Hostile Vehicle Mitigation, barriers (doors, turnstiles, structures, fences, walls), communications, search equipment, human factors (space for searching, monitoring stations etc.) response support (tracking) and PPS network with their support systems (power, sensors, cables, servers, cameras). Then where these capabilities are required against the building and room layout. These capabilities should add depth and difficulty thereby frustrating an adversary by target hardening that might include disguising the assets. It might also include channelling or funnelling an adversary to specific areas for a response or adding complexity to their attack plans.

- Capabilities, together with the effect sought at a given place in the plant, could be described in sufficient detail to enable the licensee to develop that basic operational requirement into more technical specifications. The RP's collection of security requirements should draw from the idea of categorisation and classification of security functions and capabilities required. In this way it would provide confidence that the security arrangement or system could achieve the desired effect.

- However, as a note of caution, there is no definitive expected level of detail required by the RP in describing their security regime. In the future, more mature GDA designs might provide the type of detail described above and offer a high level of granularity in terms of defining requirements. In other GDAs, the RP's evidence might not be based on that level of detail, and this may not be possible nor advisable as these are likely to be licensee choices. In most cases the development of conceptual security regime, in terms of exact

technology, is for the licensee as such technology will change over time. Nevertheless, security categorisation and classification (KSyPP 5), together with national and international codes and standards (KSyPP 6), should be used in describing the security regime even if detailed requirements are deferred until later.

- The RP's conceptual security design should clearly reference RGP, so the claims are evidenced. The use of UK national authorities, such as CPNI and the NCSC, should be part of the RGP mix, together with relevant international and national standards. In some cases, research and academic sources might be used to substantiate claims.

ASSUMPTIONS

10. It is accepted that the RP could claim that certain security features, that add to the necessary 'defence in depth' expected, could be placed outside the buildings in GDA scope. That might include barriers with means to achieve specific security 'functions' and address the DBT. The RP might argue that systems placed outside GDA scope, but within the anticipated site envelope, are part of the case for meeting the 'outcome' in their GDA arguments. This is accepted, but would need to be recorded, and discussed with the future licensee as they subsequently develop their security plan for site licence grant. Such assumptions need to be adequately argued within the Tier 2 documents, formally captured in submissions and the principle explained in the GSR security case or similar documents.

TOPICS FOR CONSIDERATION

11. Towards the latter part of any GDA process, ONR will begin to target selective areas and topics that would be sampled as part of any deeper assessment. At this juncture in GDA the expectation is that the GSR 'capstone' document' and Tier 2/3 documents have been submitted and reviewed by ONR. Also, some of these topics might be more relevant to relatively mature designs (and any small modular reactor design that incorporates security features in its novelty). Therefore, the RP's design already has security measures incorporated in its initial submissions. These are some of the likely general topic areas and 'question sets' for sampling and examination with the RP dependent on the design's maturity and the GDA approach jointly agreed by RP and ONR. This list is offered as a guide and not a 'tick list'. Some topic areas might realistically be for a licensee to consider especially when the construction is significant in terms of time and complexity.

- **'Secure by Design' and how it has been applied within GDA.** This might include:

    - What methodology has been applied?
    - What success has the RP had with the designers as a result of understanding the risk posed by the DBT to the nuclear inventory, critical safety systems and other assets that need protection from sabotage and theft?
    - Has the RP identified safety features that benefit security by way of reducing the radiological risk off-site such has barriers, redundancy, separation and passive safety?
    - Accordingly, is it possible to reduce the radiological risk and hence the sabotage consequences to a new level? That in turn could affect the associated SyAPs outcomes, related security postures and hence the security concept offered for consideration.

- **Design and Plant Information.** An explanation of how the buildings in scope are considered in terms of protected area, inner areas, vital areas, stores, access control points, central control rooms, security control rooms and others. What security features might be outside the protected area and towards the limited access area? For this TAG TAST-GD 6.3 refers.

- **Physical and Cyber Protection Systems and integration with plant operations and safety measures**. Again, the level of detail chosen for sampling depends on the maturity of the design in meeting UK expectations. This might include several topics, and some are more relevant to 'secure by design':

    - What is the requirement for conducting plant operations? Consideration of access requirements and footfall together with working hours and outages.
    - Does safety redundancy and segregation provide benefits to security risk reduction?
    - Can safety and security alarm monitoring team-up?
    - Do radiation protection measures, including walls and barriers, aid security?
    - How do emergency arrangements affect security and access management?
    - How do security power requirements affect the electrical power requirements for the plant?

- **Access Management within the buildings in scope.** This might include:

    - Limitations imposed by operations.
    - Vehicle access into the plant within scope.
    - Assets to protect and adversary pathways by DBT elements.
    - Where to deliver security functions of detect, delay etc. This could be specific in simple designs but in large plants it may be limited to a framework or methodology to deliver these functions.
    - Capabilities to deliver the functions including barriers, CCTV, IDS, AACS, Lighting, HVM etc.
    - Alarm station or security control room.
    - Vehicle and personnel searching areas.
    - Power, UPS and standby power requirements.
    - Zoning to limit access including the idea of vital areas, inner areas, and protected areas.
    - Related standards and RGP.

- **Control and Communications.** This might include making provision for:

    - Alarm station location.
    - Anticipated response force tactical operations and impact on design (including basing, detection, assessing, tracking, access control, funnelling).
    - A resistant PPS network and support systems that link sensors and cameras via infrastructure to servers and workstations.
    - Power requirements including cabling.

- **Assumptions related to Licensee responsibilities.** This might include:

- In order to achieve the outcome and response sought, has the RP drawn on anticipated additional depth outside the buildings in GDA scope?
- Has the RP identified space for security functions of detect, delay, assess etc.?
- What aspects of technology may change over the construction period?

- **Cyber – protection of nuclear technology and operations.** Might include:

  - Transferring the output from the cyber security risk assessment work into the Tier 2 documents to reflect expectations in the relevant SyAPs.
  - Demarcation between 'cyber safety' and cyber as a vector for sabotage either separately or in combination with physical and insider actions.

LEVEL OF DETAIL

12. Within safety, ONR assessors would want to see compelling evidence of a 'golden thread' ranging from analysis of risk to engineering solutions. Within the Reference Design, some safety assessors have something tangible on which to base their assessment. For security, the existing systems on the Reference Design may not provide a ready solution as they maybe predicated on meeting other regulatory regime requirements or do not anticipate the need to attempt a 'secure by design' approach but add security on to the site progressively during construction. Within security, the RP should provide the potential licensee with enough detail so the latter might then draft more technical specifications drawn from an outline requirement statement within GDA Tier 2 documents. For example, while a need for 'detect' should be identified by location, it might also be possible to describe a type of sensor by way of performance with the details left for the licensee to consider. However, in most cases in GDA, ONR assessors would like to see a line of logic from security functions, that meet SyAPs specified outcomes and indicative postures, to a description of their delivery at a given location. That would be, reflecting a graded approach, commensurate with the risk. The 'effect' sought should be described in a way that specifies the capability needed to deliver that result. Capability has human, technical and procedural elements and, while all components of capability should be considered, the more technical aspects should be stated. The level of detail provided by the RP, by way of security requirements, will depend on the maturity of the design and what should be a licensee's decision.