

RECONCEPTUALISING “FACILITY-SECURITY DESIGN” (FSD)

Tariq Ahmad

Keywords: *critical infrastructure, security engineering, disaster management planning*

On 27 June 2017, AP Møller-Maersk, one of the world’s largest shipping companies, was struck by NotPetya, a malware initially resembling ransomware but subsequently understood to function as a destructive wiper. The attack disrupted the company’s information systems across its global operations, affecting the data and services required for routine business functions.¹ The scale of the disruption exposed an important characteristic of a highly interconnected organisation: the geographical separation of facilities did not necessarily provide separation from a common failure. The recovery of Maersk’s systems depended, unexpectedly, on a server in Ghana that had remained offline during the attack. Because it was disconnected from the affected network, the server retained a copy of information that could be used to help restore operations. A component that had not been deliberately designed as the organisation’s principal recovery mechanism therefore became critical precisely because it did not share the failure pathway of the systems intended to support the business. The consequences extended beyond Maersk’s corporate systems. At Jawaharlal Nehru Port in Mumbai, disruption to the Gateway Terminals India facility operated by APM Terminals, Maersk’s terminal arm, affected container-handling operations. The consequences, however, did not remain confined to the terminal function, either. Disruption to cargo-handling contributed to landside congestion and the diversion of traffic to other ports, propagating the effects of a failure within one operational function into a wider logistics system.²

The episode, therefore, highlights a point that extends well beyond cyber security. The systems that failed were not necessarily the systems that ultimately experienced the greatest operational consequence. Nor did the apparent boundaries of the affected systems correspond to the boundaries of the functions that depended upon them. A failure in an information system could propagate through terminal operations, landside traffic, and wider logistics, because these functions were connected through dependencies that extended beyond their immediate organisational or physical boundaries. This is a recurring problem in the protection of critical infrastructure. Security arrangements are necessarily designed around assumptions about how threats will emerge, how protective measures will operate, and which functions will remain available when individual components fail. Yet the effectiveness of a security arrangement ultimately depends upon those assumptions continuing to hold. A deliberate adversary, unlike an accidental hazard, can actively seek vulnerabilities in the way a system has been protected and can exploit conditions that the security architecture did not anticipate.

¹ Sean Steinberg, Adam Stepan, and Kyle Neary, *NotPetya: A Columbia University Case Study* (New York: Columbia University School of International and Public Affairs, 2021), <https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf>

² United Nations Conference on Trade and Development (UNCTAD), “Case Study 16: Jawaharlal Nehru Port Trust (JNPT), India”, in *Building Capacity to Manage Risks and Enhance Resilience: A Guidebook for Ports*, 76, <https://resilientmaritimelogistics.unctad.org/guidebook/case-study-16-jawaharlal-nehru-port-trust-jnpt-india>

This raises a more fundamental question relevant to the concept of “security-by-design”: *What assumptions must remain true for a security architecture to perform its intended function, and what happens when one of those assumptions is deliberately or inadvertently invalidated?*

The question is particularly relevant as the maritime sector increasingly adopts this “security-by-design” approach. Recent policy discussions on port security have placed greater emphasis on integrating security considerations into the design and development of facilities. The challenge, however, is not only to incorporate security measures into a facility’s spatial, architectural, or operational design. It is to establish a coherent design logic through which the assumptions, the dependencies, and the functional consequences underpinning those measures are identified and carried through the design of the facility as a whole.

This article explores what one might call the “upstream layer” of this “security-by-design” concept, namely, the design of the security concept itself. It proposes an approach in which the security of a critical facility is considered not merely as a collection of protective measures, but as a system of functions, dependencies, and assumptions, whose validity must be examined throughout the design and evolution of the facility.

Security-planning for a port sits at the intersection of several forms of planning. Port operations determine how vessels, cargo, vehicles, personnel, and equipment move through the facility, while spatial and architectural planning organises the physical infrastructure required to support those functions. Security planning introduces requirements governing who, what, and under which conditions these spaces and functions can be accessed, while also providing measures for detection, protection and response. The resulting security arrangements, therefore, interact with the operational and physical organisation of the port, rather than existing separately from them.

A fundamental principle through which these requirements are commonly organised is **zoning**.³ A port facility is divided into areas with different levels of access and control, with interfaces between them regulated through measures such as identification, screening, barriers, and surveillance. The same principle can extend beyond physical space. Operational processes can be organised around controlled interfaces between different functions, while information systems can apply analogous principles through differentiated levels of access, authentication, and network segregation. In each case, the underlying objective is to establish boundaries within which particular activities, assets, and users, can be controlled. Zoning, however, does not, in and of itself, constitute a security architecture. A zone can be secured only insofar as the controls governing its boundaries and internal functions continue to operate as intended. Access control may, for instance, depend upon electricity, communications, identification systems, trained personnel, and supporting procedures; surveillance may depend upon networks, power, and command functions; and emergency response may depend on access routes, communications, and the continued availability of personnel and equipment. These dependencies can cross the very boundaries that the security arrangement seeks to establish.

The distinction is therefore important: **zones and security controls are components of a security architecture, but they are not the architecture itself**. The effectiveness of the overall arrangement depends not only upon whether individual controls are present, but also upon the assumptions, dependencies, and relationships, which allow these controls to function together. It is this underlying design logic that the following cases illustrate.

³ Department for Work and Pensions, Security Standard: Physical and Electronic Security (Part 1) (London: UK Government, 2022), sec. 12, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118262/dwp-security-standard-physical-and-electronic-security-part-1-v1.1.pdf

In the Indian context, these dimensions of security are addressed through a distributed body of codes, standards, guidelines, and statutory requirements. The “International Ship and Port Facility Security (ISPS) Code”⁴ provides the principal international basis for minimum maritime security requirements, while additional requirements may arise through codes formulated and promulgated by the “Bureau of Indian Standards” (BIS) and other suchlike standards relating to construction⁵, structural design⁶, building services, electronic systems, and cyber security.⁷ Requirements and guidance issued by the Ministry of Home Affairs (MHA)⁸ may provide further considerations, particularly for the protection of critical facilities. Spatial and facility-design considerations are also addressed through instruments such as the “National Building Code of India” and associated guidance on asset and facility management.⁹ These instruments contribute to different dimensions of facility security, including physical and spatial protection, operational arrangements, and the protection of supporting systems.¹⁰

The resulting framework is, therefore, not necessarily deficient because relevant requirements are absent. Rather, security requirements are distributed across instruments that originate from different institutional and technical domains. A facility may consequently satisfy the requirements applicable to individual aspects of security, while the assumptions and dependencies connecting those aspects remain implicit. This distinction is central to the argument developed below. In other words, the need is not necessarily for another set of security requirements but rather, for a facility-level reference through which existing requirements can be understood and developed as a coherent security design.

When Security Premises Fail

The limitations of a control-based approach become clearer when security arrangements are examined through incidents in which the assumptions underlying them were invalidated. The nature of these assumptions varies. They may concern where a threat can originate, how an adversary is expected to behave, which activities are considered legitimate, or which supporting systems are expected to remain available. The resulting failures need not involve the direct defeat of a security-control. In some cases, the control continues to operate as designed while the condition upon which its effectiveness depends has changed.

The 2013 attack on the Metcalf transmission substation in California illustrates the distinction between a security boundary and a threat boundary. The facility had perimeter security intended to restrict unauthorised physical access, but the attackers remained outside the perimeter and used rifle fire to damage

⁴ International Maritime Organization, *International Ship and Port Facility Security (ISPS) Code*, adopted under chapter XI-2 of the *International Convention for the Safety of Life at Sea (SOLAS)*, 1974, 2003.

⁵ Bureau of Indian Standards, *National Building Construction Standards 2026 (NBCS 2026)*, SP 7:2026 (New Delhi: Bureau of Indian Standards, 2026).

⁶ Bureau of Indian Standards, *Criteria for Blast Resistant Design of Structures: Part 1 Above-Ground Explosions (First Revision)*, IS 4991 (Part 1):2024 (New Delhi: Bureau of Indian Standards, 2024).

⁷ Indian Computer Emergency Response Team *CERT), Ministry of Electronics and Information Technology, Government of India, Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, 28 April 2022, <https://www.cert-in.org.in/Directions70B.jsp>

⁸ Ministry of Home Affairs, Government of India, *Revised Draft Guidelines on Security of Non-Major/Minor Ports*, 2022, <https://www.scribd.com/document/1063361190/Revised-Draft-Guidelines-on-Security-of-Non-Major-Ports-2022-Reg-1>

⁹ Bureau of Indian Standards, *National Building Code of India: Part 12 Asset and Facility Management (Preliminary Draft*, October 2024), <https://www.scribd.com/document/866377493/Draft-NBC-Part-12>

¹⁰ AECOM India Private Limited, *Consultancy Services for the “Preparation of Detailed Project Report and Port Planning for the Development of Port at Astaranga Area, Puri District, Odisha”*, revised offer, 24 August 2023, <https://www.scribd.com/document/788234393/1-AECOM-Techno-Commercial-Offer-NECL-24-08-2023-Draft>

critical equipment.¹¹ The physical boundary therefore did not coincide with the distance from which the facility could be effectively attacked. The incident illustrates a broader problem in security design: a protected zone does not necessarily define the full spatial extent of the threat to the functions within it.

The terrorist attacks of 11 September 2001 upon the USA illustrate a different form of premise failure. Hijacking was a known threat, and aviation security arrangements had been developed around that threat. However, the established conception of hijacking was principally associated with the seizure of an aircraft for purposes such as negotiation or diversion, rather than its deliberate use as a weapon.¹² The attack, therefore, did not introduce an entirely unknown threat; it altered the purpose for which a known threat could be operationalised. The security architecture had been developed around one interpretation of the threat while the adversary exploited another.

A similar issue arises in the maritime environment, where security must operate alongside legitimate activity. The 2000 attack on the USS Cole demonstrated the difficulty of distinguishing a hostile approach from the normal movement of vessels within a functioning harbour environment. A security system cannot simply exclude every small craft from its operational environment without also preventing the legitimate activities upon which maritime operations depend. The problem is therefore not only controlling access to a protected zone, but determining which activities and interfaces must remain permissible while retaining the ability to identify and respond to hostile use of those same interfaces.¹³

The same principle extends to technological separation. The Slammer Worm incident of 2003 and the later Stuxnet operation demonstrated that nominally isolated or protected systems could remain exposed through pathways outside the boundary assumed by the security architecture.¹⁴ An air gap, network segregation or other technical boundary is, therefore, not an independent security function in and of itself. Its effectiveness depends upon the assumptions surrounding how information, equipment, software, and people can cross that boundary. The relevant question is not simply whether a system is isolated, but whether the conditions required for that isolation to remain meaningful have themselves been secured.

The 2021 Colonial Pipeline incident demonstrates a further distinction between direct compromise and functional consequence. The ransomware attack affected the company's information-technology systems, with no identified infection of the operational technology systems controlling the physical pipeline.¹⁵ Nevertheless, the company suspended pipeline operations because it could not establish sufficient confidence in the integrity of the systems and interfaces supporting those operations. The physical system,

¹¹ Paul W Parfomak, *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?*, Congressional Research Service Report R45135 (Washington, DC: Congressional Research Service, 2018), <https://www.everycrsreport.com/reports/R45135.html>

¹² National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, 2004), <https://govinfo.library.unt.edu/911/report/index.htm>

¹³ Raphael Perl and Ronald O'Rourke, "Terrorist Attack on USS Cole: Background and Issues for Congress", *Congressional Research Service Report RS20721* (Washington, DC: Congressional Research Service, 2001), <https://www.history.navy.mil/content/history/nhhc/browse-by-topic/ships/modern-ships/uss-cole/terrorist-attack-on-uss-cole-background-and-issues-for-congress.html>

¹⁴ Beyza Unal and Roger Brunt, *Cybersecurity by Design in Civil Nuclear Power Plants* (London: Chatham House, 24 July 2019), <https://www.chathamhouse.org/2019/07/cybersecurity-design-civil-nuclear-power-plants/introduction>

¹⁵ Joseph Blount, "Testimony of Joseph Blount, President and Chief Executive Officer, Colonial Pipeline Company", delivered before the United States Senate Committee on Homeland Security and Governmental Affairs, 8 June 2021, <https://www.colpipe.com/news-insights/media-resources/post/hearing-before-the-united-states-senate-committee-on-homeland-security-governmental-affairs-testimony-of-joseph-blount-president-and-chief-executive-officer-colonial-pipel/>

therefore, entered a degraded state without being directly compromised. The incident illustrates how the security or integrity of one system can become a prerequisite for the continued operation of another.

These examples become particularly significant when the threat itself changes its method of reaching a protected function. Emerging technologies such as unmanned autonomous systems (UAS) can alter the spatial relationship between an attacker and the target. The 2025 Ukrainian Operation Spider's Web, for example, demonstrated a form of attack in which drones were introduced covertly into the vicinity of their eventual targets rather than approaching those targets solely from the direction of the front line. The significance for security design is not simply that drones represent a new threat. Drones were already a recognised threat. The more consequential issue is that a known threat can be operationalised through a pathway that changes the assumptions on which the existing protection of a facility is based.¹⁶

Taken together, these cases point to different categories of security premise. A security architecture may make assumptions about the **objective** of an adversary, the **pathway** through which a threat can reach a target, the **boundary** within which security controls are effective, the **legitimacy of activities** occurring around the protected function, or the **availability of supporting systems** on which security depends. The specific assumptions differ between facilities and threats, but the underlying problem is common: the effectiveness of a security arrangement is conditional upon a set of circumstances remaining valid.

The problem, therefore, is not simply insufficient imagination. Nor can it be resolved by attempting to enumerate every possible attack. The more fundamental question is whether security planning contains a systematic process for identifying the assumptions on which the existing architecture depends and testing their validity. Given an existing threat, what assumptions does the security architecture make about the adversary's objective, method, pathway and constraints? What functions and dependencies must remain available for the security arrangement to operate as intended? Which of these conditions can be invalidated by a deliberate, accidental or natural event? And when one of them is invalidated, what degraded state does the wider facility enter? These questions shift the focus from individual security controls towards the design logic that connects them.

The Gap

The effectiveness of a security arrangement is conditional upon the premises within which it is expected to operate. A restricted zone, for example, may be secured through controlled access points, surveillance, and screening of personnel. Yet each of these measures depends upon conditions outside the immediate control point: personnel must remain available and vigilant, identification systems must function, communications must remain available, and the power and other utilities supporting the systems must be maintained. A failure of one of these enabling conditions can, therefore, compromise the security function without the security control itself necessarily failing. These dependencies become more significant as security arrangements are distributed across a complex facility. Spatial planning divides the facility into zones and regulates their interfaces; operational planning determines how people, vehicles, vessels, and materials, move between them; and security planning establishes controls over these movements. The systems supporting these arrangements, however, do not necessarily follow the same boundaries. A security function within one zone may depend upon power, communications, information systems,

¹⁶ National Defense University of the Republic of Kazakhstan, *Bulletin of the National Defense University of the Republic of Kazakhstan*, No. 3 (106), September 2025, <https://nuo.edu.kz/wp-content/themes/nuoportall/files/%D0%A5%D0%90%D0%91%D0%90%D0%A0%D0%A8%D0%AB%D0%A1%D0%AB3-2025.pdf>

personnel or response capabilities located elsewhere. The security boundary and the functional boundary are, therefore, not necessarily coincident.

The problem is further complicated when a condition supporting security is invalidated by an event that was not itself conceived as a security threat. A cyclone or *tsunami* may disrupt power, communications, access routes, or surveillance systems; a fire or an industrial accident may restrict movement or displace personnel; an emergency evacuation may alter the normal population- and movement patterns upon which access-control arrangements depend. In each case, a security measure may remain physically intact even while the conditions that allow it to perform its intended function have changed. The resulting effect may extend beyond the zone or system in which the initiating failure occurred. The challenge becomes particularly significant in the maritime domain. Maritime facilities operate at an interface between controlled land-based infrastructure and an inherently less controllable marine environment, limiting the extent to which access and approach pathways can be regulated. At the same time, disruption to maritime functions can propagate beyond the facility through vessel movements, cargo flows, navigational access and connected landside infrastructure. These characteristics increase the consequences of any subversion of the assumptions on which a facility's security architecture is based.

Existing security planning can address many of these vulnerabilities within individual systems, zones or functional areas. Security assessments can identify weaknesses, and contingency arrangements can provide additional layers of protection or response. The difficulty is that such planning does not necessarily establish a common, facility-level logic through which the premises and dependencies of these arrangements are identified and carried consistently into the design of their constituent systems. This distinction is important. The question is not simply whether each subsystem has been adequately secured, but whether the assumptions on which the security of one subsystem depends remain compatible with the assumptions of the wider facility. A subsystem may therefore be secure within its defined boundary while relying on a function, resource or condition outside that boundary that has not been considered part of its security design. Conversely, a higher-level security requirement may depend upon several lower-level systems, each of which may introduce further assumptions of its own.

This creates a design problem that cannot be resolved simply by adding further security controls or by attempting to anticipate every possible scenario.¹⁷ What is required is a means of establishing, before the constituent systems are fully designed, the fundamental security logic of the facility: what security is intended to achieve, what conditions must remain true for it to function, what functions and systems it depends upon, and how these requirements are to be reflected in spatial, operational and security design. In other words, the missing element is not necessarily another security measure, but an upstream reference for security-design. Without such a reference, the security of individual zones and systems may be designed correctly within their respective boundaries while the assumptions and dependencies connecting them remain implicit. It is this gap between the security of constituent systems and the security logic of the facility as a whole that necessitates a facility-level security concept.

Reconceptualising Facility-Security Design (FSD)

The cases discussed do not necessarily indicate poor planning or failure of individual security measures. In many instances, the systems involved operated as intended within the conditions for which they were designed. The difficulty arose when those conditions were no longer valid, or when a failure in one system

¹⁷ Rick Nunes-Vaz and Steven Lord, "Designing Physical Security for Complex Infrastructures", *International Journal of Critical Infrastructure Protection* 7, No. 3 (2014): 178–192, <https://doi.org/10.1016/j.ijcip.2014.06.003>

affected the assumptions on which another depended. The challenge, therefore, is not to anticipate every possible scenario or to model every possible cascade, but to establish the fundamental logic by which security is intended to function across the facility.

This requires an ‘upstream reference’ for security design. At the highest level, a security doctrine or intent establishes what the facility is expected to protect and the fundamental approach by which security is to be achieved. This can then be translated, at the facility level, into a common security concept that identifies the relevant threat environment, critical functions, operating environment, principal premises and assumptions, and the dependencies through which security is to be delivered. These considerations provide a basis from which the spatial, operational and security dimensions of the facility can be developed coherently rather than as independent design exercises.

Such a concept would not replace existing security plans or require every subsystem to replicate the facility-level analysis. Instead, it would provide the common reference from which the security requirements and assumptions of individual systems and zones can be derived. As the facility is progressively disaggregated into constituent systems, these systems can identify their own dependencies and assumptions while remaining traceable to the security requirements established at the facility level. In this way, security design can retain a common logic even where its implementation is distributed across different disciplines, zones and systems.

This provides the framework for reconceptualising “Facility-Security Design” (FSD) by generating a **documented facility-level reference** that translates security intent into an explicit representation of the facility's protected functions, threat environment, security premises, dependencies, boundaries and design principles. The FSD provides the common basis from which subordinate security architecture, plans and requirements can be developed, while providing a reference against which subsequent design decisions and modifications can be traced and evaluated. In this conceptualisation, the FSD is, therefore, not merely another layer of security controls. It is the mechanism through which the security of the individual parts can remain connected to the security logic of the facility as a whole.

Figure 1 illustrates a schema of incorporating FSD into security-planning and further extending it into the domain of disaster-risk reduction. At the highest level, a security doctrine establishes the governing principles by which security is to be approached. These principles are translated into a facility-specific security intent defining what security is expected to achieve. The intent can then be developed, at the facility level, into a common security concept that identifies the relevant threat environment, critical functions, operating environment, principal premises and assumptions, and the dependencies through which security is to be delivered.

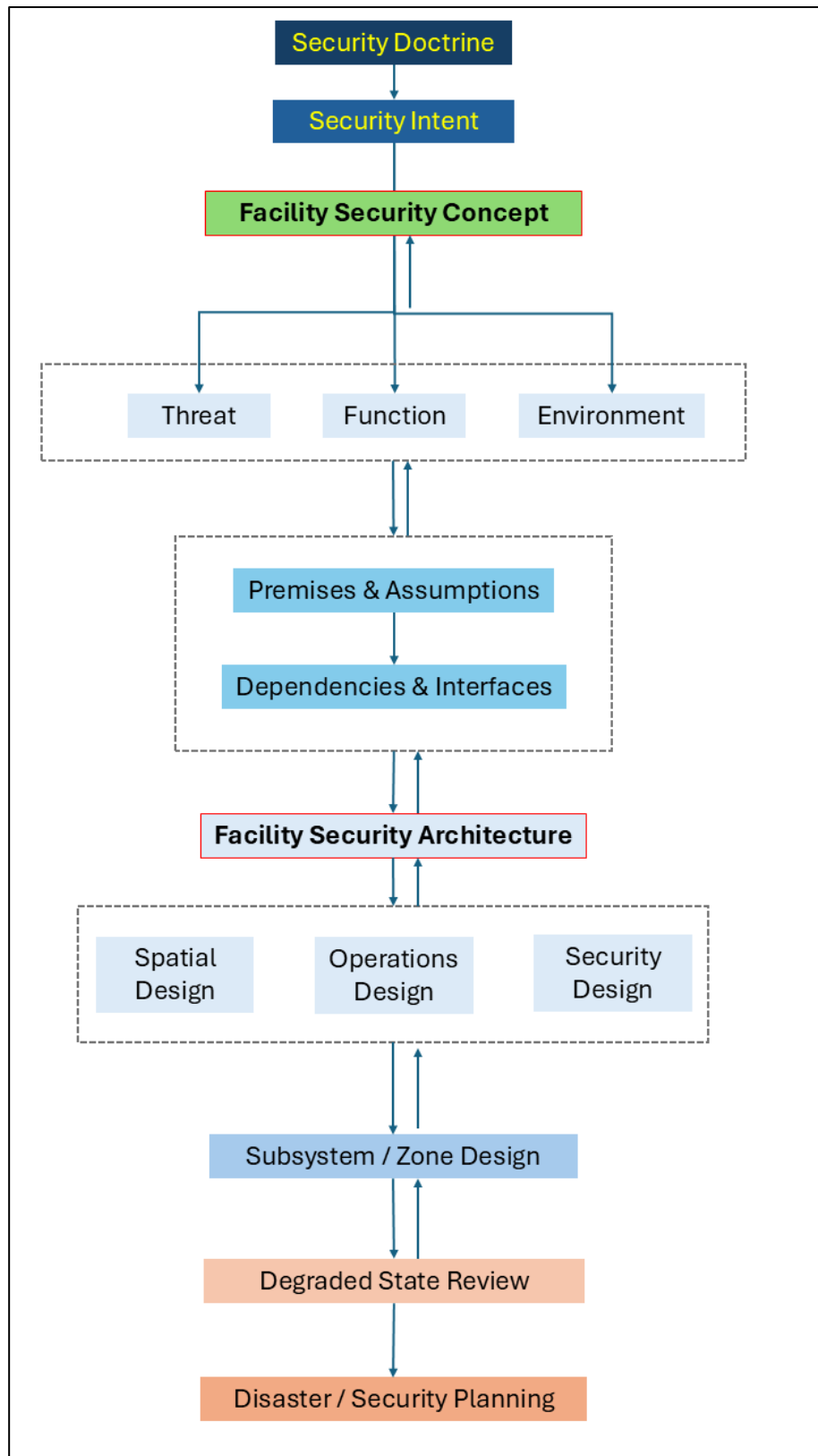


Fig 1: Schema for FSD implementation

Source: Author

The FSD provides the documented reference through which a facility's security doctrine and intent are translated into a coherent security design. It establishes, at the facility level, what must be protected, the functions through which protection is to be achieved, the relevant threat environment, **the principal security premises and assumptions**, and the dependencies and interfaces upon which those arrangements rely. Rather than prescribing individual security measures, the FSD establishes the design-logic from which the facility's security architecture and subordinate security and disaster management plans can be developed.

The FSD also provides **traceability across levels of planning**. Requirements and assumptions established at the facility level can be carried into individual zones, functions, systems and operational plans, while remaining referable to their originating security intent. This allows a subordinate plan or design decision to be examined not only for compliance with its immediate requirements, but also for consistency with the security logic of the facility as a whole. An important function of the FSD is, therefore, the explicit documentation of assumptions and dependencies. These provide the basis for reviewing degraded states: conditions in which one or more functions, systems, utilities, access controls or other enabling elements cease to operate as intended. The degraded-state review examines whether the security concept remains valid under such conditions, what functions or protections are affected, and whether the resulting condition introduces a requirement that was not reflected in the existing design.

The relationship is consequently not purely hierarchical. FSD provides the basis for subordinate security and disaster planning, while the findings of degraded-state review provide feedback into the FSD and, where necessary, the underlying security doctrine or intent. This creates a traceable loop through which the security concept can be reviewed as the facility, its threat environment, dependencies and operating conditions evolve. The FSD is intended to provide a common reference across the various disciplines and systems contributing to facility security. Its accessibility need not, however, imply disclosure of the detailed security arrangements of the facility. It operates at a level of abstraction appropriate to the facility as a whole, establishing the security intent, protected functions, principal threats, dependencies, assumptions and design principles. Detailed configurations, vulnerabilities, response procedures and system-specific security measures can remain within the subordinate plans and systems to which they relate. Thus, a designer working on one system can understand the security conditions and dependencies that their system must satisfy without necessarily having access to the detailed security arrangements of other systems.

Way Forward

It is reiterated that the conceptual gap identified above does not necessarily require the creation of another layer of security regulation or a uniform methodology for all critical facilities. The immediate requirement is to recognise, within security planning frameworks, the need for a facility-level reference that explicitly establishes the security intent, premises, dependencies and design principles from which subordinate arrangements are developed. Such a principle could be incorporated into existing security planning frameworks through appropriate guidance, standards or model provisions, with the level of detail and form of the FSD adapting to the nature and sensitivity of the facility.

A second opportunity lies in integrating the FSD with planning for disaster risk-reduction. The conditions that can invalidate a security premise are not necessarily malevolent. Natural hazards, technological accidents and operational disruptions can disable utilities, restrict access, displace personnel or alter normal movement patterns in ways that affect the assumptions underlying security arrangements. Model Disaster Management Plans and ministerial DMPs can therefore recognise the FSD as a reference for examining how degraded states affect security functions, while security planning can use the same process to identify

conditions in which disaster scenarios may invalidate security premises. This would establish a common interface between security planning and disaster management without requiring the two to become a single planning instrument.

Once such a relationship is established, review and traceability should operate in both directions. Security assessments should not only examine whether subordinate systems and controls continue to satisfy the requirements derived from the FSD, but also identify whether changes to those systems, newly recognised dependencies or observed degraded states have altered the premises on which the FSD was based. Significant changes could, therefore, trigger a review of the FSBS and, where necessary, even the security intent or doctrine from which it was derived. The FSD would consequently function as a maintained reference rather than a static document produced only at the beginning of a project.

There may also be value in making selected, non-sensitive elements of the security concept available beyond the immediate facility-design team. A sufficiently abstract representation of the facility's security objectives, functional dependencies, and design principles, could allow architects, engineers, planners, researchers, and other stakeholders, to incorporate relevant security considerations without requiring access to detailed security plans or system configurations. Where appropriate, such publicly accessible material could also provide a basis for wider research and professional input while preserving the confidentiality of facility-specific vulnerabilities and protective arrangements. The distinction between sharing the security concept and disclosing the security system is important: the former can support security-by-design, while the latter may itself create security risks.

Conclusion

The protection of critical infrastructure is often expressed through the accumulation of security measures: controlled access, surveillance, barriers, authentication, redundancy, response arrangements, and other protective systems. These measures remain essential, but their effectiveness is conditional upon the assumptions upon which they have been designed. An adversary may alter the objective or pathway of an attack; a technological development may create a new means of reaching a protected function; or a natural or accidental event may disable a dependency on which a security arrangement relies. In each case, the resulting vulnerability may lie not in the absence of a security measure, but in the assumptions connecting otherwise adequate measures into a functioning security architecture.

“Security-by-design” therefore requires consideration beyond the design of individual controls or zones. It requires a means of establishing and preserving the logic that connects the security of individual systems to the security of the facility as a whole. The Facility-Security Design concept provides such a reference by explicitly documenting the security intent, protected functions, premises, dependencies, and design principles, from which subordinate security arrangements can be developed and against which they can subsequently be reviewed.

The value of this approach lies particularly in its traceability. As a facility is progressively disaggregated into zones, functions, and systems, the increasing specificity of security requirements need not result in fragmentation of the underlying security logic. Each lower-level arrangement can remain referable to the facility-level concept, while changes and degraded states can be traced upwards to determine whether the original premises remain valid. The same relationship can connect security planning with disaster management, recognising that events not intended as security threats can nevertheless invalidate the conditions upon which security depends.

The proposed approach does not seek to predict every possible attack or eliminate every possible failure. Nor does it imply that all security information should be consolidated into a single document or made universally accessible. Its purpose is far more fundamental: to make the assumptions connecting security measures explicit, documented, and traceable across the hierarchy of facility planning. Incorporating this principle into security planning frameworks and establishing its interface with model and ministerial disaster management plans, would provide a basis for security assessments to examine not only whether individual measures remain effective, but whether the security logic connecting them remains valid.

In this sense, the FSD represents an ‘upstream layer’ of “security-by-design”: not another security control, but a common reference through which security intent can be translated into design, design can be translated into subordinate plans, and experience from degraded states can be traced back to the assumptions from which the security system was originally conceived.

About the Author

Mr Tariq Ahmad is a Research Associate at the National Maritime Foundation. His research focuses upon port adaptation, disaster- and climate-change resilience, maritime spatial planning, and the “blueing” of the economy. His background is in architecture and spatial planning (urban & regional). He may be contacted at rsor1.nmf@gmail.com.