# **Analysis of Security-Related Application Conditions (SecRACs) in the TMF Interim Cybersecurity Case, Aligning with TS 50701 Principles**

## **I. Understanding Security-Related Application Conditions (SecRACs) in the Context of TS 50701**

### **A. Definition and Purpose of SecRACs as per TS 50701**

The standard TS 50701, which pertains to cybersecurity for railway applications, introduces the concept of Security-Related Application Conditions (SecRACs). A SecRAC is defined as 1:

1. Technical countermeasures introduced outside of the considered System under Consideration (SuC), or
2. Organisational and procedural countermeasures, or
3. Any combination of points 1 and 2.

This definition is fundamental as it provides a formal mechanism to address cybersecurity requirements that cannot be, or are not yet, met directly within the boundaries of a specific SuC. This is particularly relevant in complex operational environments like railways, where systems may be in various lifecycle stages or subject to specific operational constraints. The CENELEC technical specifications CLC/TS 50701:2023 2 and its predecessor CLC/TS 50701:2021 3 consistently refer to "Security-related application conditions" (e.g.3; 2), underscoring their integral role in the standard's framework.

The concept of SecRACs is closely aligned with the principle of "compensating countermeasures" found in related standards, notably the IEC 62443 series for industrial automation and control systems security. IEC 62443 acknowledges that "The standard foresees that a security requirement can be addressed either directly or by a compensating countermeasure. The concept of compensating countermeasures allows a certain security level to be reached even if some requirements cannot be implemented directly".4 This highlights that SecRACs are not merely passive conditions but active risk management instruments. They enable operations to continue by formally acknowledging and addressing security gaps that arise when an "ideal" or fully self-contained security posture within the SuC is not immediately achievable. This can be due to factors such as the integration of legacy systems, phased project deployments (as seen in the Torbanlea Manufacturing Facility (TMF) interim case), or dependencies on external entities or services.

The three distinct categories of SecRACs inherently support a defence-in-depth security strategy. Technical countermeasures introduced outside the SuC establish an external protective layer. Organisational and procedural countermeasures address the critical human and process elements of security. The option to combine these allows for a multi-faceted and resilient approach, moving beyond reliance on single points of control. This aligns with broader cybersecurity philosophies emphasizing layered security, as also noted in TS 50701 regarding defence in depth.2

### **B. The Imperative for SecRACs in Interim or Constrained Operational Phases**

The practical necessity for SecRACs becomes particularly evident during interim operational phases, such as system commissioning. The "CQ20 Torbanlea Cybersecurity Case" (referred to as the TMF Cybersecurity Case) explicitly states, "This report specifically addresses the cybersecurity posture for the duration of this interim phase, which is distinct from the final operational network architecture".1 It further clarifies, "As a consequence of the interim nature of this phase, we rely on the use of Security-Related Application Conditions (SecRACs) to guide the testing phase...".1

During such interim periods, the complete suite of technical cybersecurity controls designed for the final, permanent operational state is often not yet fully implemented, configured, or verified. SecRACs, therefore, become essential compensating measures to maintain an acceptable level of security tailored to the limited duration and specific scope of these activities. The TMF Cybersecurity Case notes that Downer "has prepared for the worst-case scenario during this commissioning phase by implementing robust administrative controls and has adopted a '3+X' isolation strategy. This approach is particularly pertinent as many of the final cybersecurity controls for the permanent network architecture are still being verified and implemented".1 This directly indicates a reliance on measures that are often procedural, organisational, or technical but external to the SuCs themselves—hallmarks of SecRACs.

The use of SecRACs can be seen as an enabler of phased project delivery. Without a formalized mechanism like SecRACs, projects could face significant delays if commissioning or other interim operations were deemed too insecure to proceed without the final security architecture in place. SecRACs allow for a structured, risk-managed progression through project milestones, such as the commissioning of Operational Technology (OT) systems, by formally acknowledging and compensating for temporary security gaps. This is crucial for maintaining project timelines and managing financial aspects in large-scale industrial endeavors. The TMF document underscores this by stating, "This interim security case is a prerequisite for commissioning activities...".1

However, the reliance on SecRACs, particularly those of an organisational or procedural nature, or those dependent on external entities (e.g., vendor attestations), shifts the nature of security assurance. The burden of proof extends beyond merely verifying a technical control within the SuC; it necessitates ensuring that the assumed conditions or external measures are genuinely in place, effective, and consistently maintained. This implies a heightened need for robust auditing, diligent oversight, and continuous monitoring of these SecRACs. Compensating controls are often temporary and require diligent validation to ensure they provide the intended level of protection.5

## **II. SecRAC Implementation in the TMF Cybersecurity Case**

### **A. Mapping TMF's Approach to TS50701 SecRAC Categories**

The cybersecurity strategy for the TMF interim phase, as detailed in its Cybersecurity Case document 1, incorporates various measures that align with the three categories of SecRACs defined in TS 50701.

1. Technical Countermeasures Introduced Outside of the Considered SuC in TMF

These are technical security measures that are not integral to the individual OT SuCs (e.g., a specific welding robot or CNC machine) but are part of the broader interim network infrastructure or external security services that provide protection to these SuCs. Examples from the TMF documentation include:

* The requirement that "The physical network design shall reflect the separation of facility and corporate networks" (TORCS-FAC-RDF-C01).1 This network segmentation is a technical control external to the SuCs it protects.
* The interim network configuration itself, which employs "".1 These features are provided by the interim network infrastructure, not by the OT systems themselves.
* A significant compensating control identified in the TMF Detailed Risk Assessment (DRA) outputs is CompensatingControl:NISTSP800-53r5AC-17(9): Disconnect/DisableAccess.1 This control, which provides the capability to rapidly disconnect or disable remote access 6, is a technical function of the supporting infrastructure rather than the SuC.

A practical consideration arises from the nature of interim solutions. The TMF Cybersecurity Case acknowledges, "it's likely that we won't know the details [of the interim network's specific hardware] by the time we submit this report".1 This implies that some interim network components and their security features (like NAT and firewalling) are relied upon as technical SecRACs without their full, detailed specifications being integrated into this specific security case document. While the SecRAC framework accommodates such reliance on external technical provisions, it underscores the critical importance of performing thorough due diligence on these external elements to ensure they provide the assumed level of security efficacy.

2. Organisational and Procedural Countermeasures in TMF

This category of SecRACs is heavily utilized in the TMF interim phase, relying on human actions, documented processes, and organisational policies rather than purely technical system functions within the SuC. These are critical when final technical controls are incomplete. Key examples include:

* The "3+X Justification Pillars" 1 are replete with such measures:
  + "Total Isolation" involves procedural enforcement of physical or logical separation.
  + "Controlled Communication" is enforced by technical firewall rules but also governed by procedural access requests and agreements.
  + The "Preventive Control Focused" approach guides the development and enforcement of Standard Operating Procedures (SOPs).
* Explicitly defined SecRACs such as SecRAC-RA-003 (Vendor Attestation) 1 are purely procedural, relying on vendor declarations and contractual obligations.
* Downer's internal policies and standards, such as DG-IT-ST031 Vendor Management Security Standard, DG-IT-ST017 Change Management Security Standard, and DG-IT-ST015 Access Control Standard 1, form a foundational layer of organisational countermeasures.
* Procedural compensating controls derived from the DRA, such as the Compensatingcountermeasure:operatingprocedurefortrainshuntingtoincludemitigationsforspoofdigitalradiomess and Compensatingcountermeasure:awarenesstrainingforstaffinvolvedintrainshuntingtoincluderiskofspoofdigitalradior 1, are also vital organisational SecRACs.

The significant emphasis on organisational and procedural SecRACs during the TMF interim phase elevates the importance of human factors. The effectiveness of the interim security posture becomes highly dependent on human diligence, comprehensive awareness training (as highlighted by the digital radio awareness training 1), and strict adherence to documented procedures. Any lapse in these human-centric controls could disproportionately undermine security compared to a final state with more robust, automated technical controls. This implies a corresponding need for heightened supervision, clear communication of these procedural SecRACs to all relevant personnel, and potentially more frequent audits of procedural compliance.

3. Combined Countermeasures in TMF

Many practical SecRACs involve a blend of technical and organisational/procedural elements. A technical control might be in place, but its configuration, management, and the processes for its use are organisational or procedural. Examples from the TMF case include:

* SecRAC-RA-001 (Just-in-Time Access) 1: While a technical system might enforce the JIT nature of the connection, the request, approval, and monitoring processes are typically procedural and organisational.
* SecRAC-RA-002 (Network Isolation for vendor remote access) 1: This combines technical network segmentation and firewall rules with organisational policies defining permissible connectivity and the procedural change management process for approvals.
* The "Controlled Communication" pillar of the "3+X" strategy 1 explicitly relies on "Firewall rules on the interim network devices" (technical) but also on the "project's communication requirements matrix and managed vendor access agreements" (organisational/procedural).

For such combined SecRACs to be effective, a strong interdependence exists between their technical and procedural components. Both aspects must function correctly and be cohesively aligned. A technically sophisticated JIT access system, for instance, provides little security benefit if the associated approval procedures are lax or easily circumvented. Conversely, stringent procedures are rendered ineffective if the underlying technical enforcement mechanism is faulty, misconfigured, or can be bypassed. This highlights the necessity for holistic validation of combined SecRACs, scrutinizing not only each component in isolation but also their interactions and interfaces.

The following table summarizes the mapping of TMF's approach to TS50701 SecRAC categories:

**Table 1: TS50701 SecRAC Categories and TMF Implementation Examples**

| **TS50701 SecRAC Category** | **Brief Definition/Description of Category** | **Specific Examples from TMF Documents** |
| --- | --- | --- |
| 1. Technical (Outside SuC) | Technical security measures implemented in the supporting infrastructure or environment, not within the SuC itself. | Interim network firewalling and NAT 1; Network separation (TORCS-FAC-RDF-C01) 1; CompensatingControl:NISTSP800-53r5AC-17(9): Disconnect/DisableAccess 1; Physical security measures (Fac\_AS03).1 |
| 2. Organisational and Procedural | Countermeasures based on policies, standards, procedures, human actions, and organisational structures. | "3+X" Pillars (Total Isolation, Preventive Control Focused, +X procedural awareness) 1; SecRAC-RA-003 (Vendor Attestation) 1; Adherence to Downer Policies (DG-IT-ST031, DG-IT-ST017, DG-IT-ST015) 1; DRA Procedural Controls for Digital Radio.1 |
| 3. Combination (Technical & Org./Proc.) | Countermeasures that integrate both technical elements and organisational/procedural aspects. | SecRAC-RA-001 (Just-in-Time Access) 1; SecRAC-RA-002 (Network Isolation for vendor access) 1; "3+X" Pillar (Controlled Communication - firewall rules + communication matrix).1 |

### **B. In-depth Analysis of Explicit SecRACs in the TMF Document**

The TMF Cybersecurity Case explicitly defines several SecRACs, primarily focused on managing risks associated with vendor access and system integration during the interim commissioning phase.1

* **SecRAC-VH-001 - Vendor System Hardening**:
  + **Description**: This SecRAC mandates that "All vendors shall perform comprehensive system hardening on their supplied equipment prior to the commencement of testing and commissioning activities." This includes removing unnecessary services, implementing secure baselines, applying patches, configuring access controls, and documenting these measures. Vendors are required to "provide evidence of completed hardening activities".1
  + **TS50701 Alignment**: Primarily Organisational/Procedural. Downer imposes a requirement on vendors (organisational) and mandates a process involving documentation and evidence (procedural). The hardening itself is technical but is performed by an external party and verified, rather than being an inherent feature of a Downer-controlled system during this phase.
  + **Purpose**: To reduce the attack surface of new vendor equipment introduced into the TMF interim environment, thereby mitigating risks from default configurations, unpatched software, or known vulnerabilities inherent in the vendor-supplied systems.
* **SecRAC-RA-001 - Just-in-Time Access**:
  + **Description**: "Remote connections must be established on a just-in-time basis and not maintained as always-on connections. Connections shall be terminated immediately upon completion of the specific commissioning task, in alignment with NIST AC-6 Least Privilege principles...".1
  + **TS50701 Alignment**: Combination. The enforcement of JIT access may involve technical mechanisms (e.g., a remote access solution that provisions and de-provisions access dynamically). However, the policy dictating JIT, the processes for requesting and approving such access, and the monitoring for adherence are organisational and procedural.
  + **Purpose**: To minimize the window of opportunity for attackers to exploit vendor remote access sessions. This reduces risks associated with compromised vendor credentials, unattended active sessions, or exploitation of the remote access infrastructure itself.
* **SecRAC-RA-002 - Network Isolation (for vendor remote access)**:
  + **Description**: "Vendor remote access connections are prohibited from accessing the Downer corporate network unless such connectivity is explicitly part of the defined testing scope and has been approved through the change management process".1
  + **TS50701 Alignment**: Combination. Technical elements include network segmentation and firewall rules that enforce this isolation. Organisational and procedural components include the policy defining the default prohibition, the criteria for exceptions, and the formal change management process for approving any such connections.
  + **Purpose**: To contain potential security incidents originating from vendor remote access activities, preventing lateral movement from a potentially compromised vendor connection or OT system into the broader Downer corporate network.
* **SecRAC-RA-003 - Vendor Attestation**:
  + **Description**: "Vendors must provide written attestation of their remote access security measures and agree to specific cybersecurity responsibilities while connected to TMF systems".1
  + **TS50701 Alignment**: Organisational/Procedural. This SecRAC relies on contractual agreements, formal declarations from vendors, and defined responsibilities.
  + **Purpose**: To establish a formal commitment from vendors regarding their security practices and responsibilities. This provides a degree of assurance and accountability, although its effectiveness is contingent on vendor diligence and the veracity of their attestations.

The reliance on vendor-centric SecRACs like SecRAC-VH-001 and SecRAC-RA-003 introduces a "trust but verify" dynamic. While these are necessary procedural and organisational steps, their ultimate effectiveness hinges on the vendor's actual implementation of the required measures and the truthfulness of their attestations. The TMF document's requirement for vendors to "provide evidence of completed hardening activities" 1 is a crucial verification step. However, the rigor and depth of this verification process are paramount; a superficial review of attestations or hardening evidence could lead to a false sense of security. This situation reflects broader challenges in third-party risk management, where an organization's security posture can be significantly influenced by the security practices of its suppliers and partners.7 The TMF document's acknowledgement that there is an "absence of a unified, Downer-managed Remote Access System (RAS) for all OT systems during this phase" 1 further emphasizes this dependence on vendor-specific security measures and their attested compliance.

The following table provides a detailed analysis of these named SecRACs:

**Table 2: Detailed Analysis of Named SecRACs in the TMF Document**

| **SecRAC ID** | **Description** | **TS50701 Category Alignment** | **Purpose/Function in TMF Interim Phase** | **Key Dependencies/Assumptions for Effectiveness** |
| --- | --- | --- | --- | --- |
| SecRAC-VH-001 | Vendors perform comprehensive system hardening on supplied equipment (remove unnecessary services, secure configs, patches, access controls) and provide evidence. 1 | Org./Procedural (Technical by vendor) | Reduce attack surface of new vendor equipment, mitigate risks from default/vulnerable configurations. | Vendor capability and diligence in hardening; Rigor of Downer's verification of evidence; Accuracy of vendor-provided information. |
| SecRAC-RA-001 | Vendor remote connections are Just-in-Time (JIT), not always-on; terminated after task completion. Aligned with NIST AC-6. 1 | Combination | Limit window of opportunity for exploiting vendor remote access; reduce risk from compromised credentials or unattended sessions. | Technical capability to enforce/monitor JIT; Clear procedures for request, approval, termination; Vendor adherence to JIT principles. |
| SecRAC-RA-002 | Vendor remote access prohibited from Downer corporate network unless explicitly approved via change management. 1 | Combination | Contain incidents from vendor access; prevent lateral movement to corporate network. | Effective network segmentation/firewall rules; Robust change management process; Clear definition of "testing scope." |
| SecRAC-RA-003 | Vendors provide written attestation of their remote access security measures and agree to cybersecurity responsibilities. 1 | Org./Procedural | Establish formal vendor commitment and accountability for security practices. | Vendor truthfulness and diligence; Clarity of contractual cybersecurity responsibilities; Enforceability of attestations/agreements. |

### **C. The Role of Assumptions as a Foundation for SecRACs**

Assumptions play a critical, foundational role in the TMF interim security case and its reliance on SecRACs. Section 9 of the TMF Cybersecurity Case explicitly states, "Controls related to Downer-provided IT infrastructure are captured as assumptions and form the foundation of the SecRACs framework".1 Section 5 of the document lists several key assumptions, such as Fac\_AS01 (consistent patch management), Fac\_AS02 (appropriate ISMS for SuC management), and Fac\_AS03 (physically secure environment).1

These assumptions are not passive statements but active pre-conditions for the effectiveness of many SecRACs. For example, if the assumption of robust physical security (Fac\_AS03) is invalid, the effectiveness of on-site procedural SecRACs or technical controls relying on physical protection diminishes significantly. Similarly, if patch management on the underlying Downer IT infrastructure (Fac\_AS01) is weak, any technical SecRACs that depend on the integrity of that infrastructure could be undermined.

Effectively, many of the assumptions listed in Section 5 1, particularly those pertaining to Downer's established security policies, procedures, and infrastructure management (e.g., Fac\_AS02: "It is assumed that the SuC will be managed using an appropriate cyber/information security management system (e.g. 62443-2-1, 62443-2-4...)"), function as high-level organisational SecRACs. They represent conditions external to the specific interim SuCs that are presumed to be true and are relied upon to contribute to the overall security posture. The entire TMF interim security case rests on the validity and continued effectiveness of these broader organisational controls. The commentary within the TMF document regarding the need to highlight "New assumptions specific for the testing phase" and to ensure that "Applicable assumptions from the DRA assumption list" are updated with validation status before testing commences 1 further underscores their active role and importance as part of the overall SecRAC landscape. If these foundational assumptions are not validated or prove to be incorrect, the integrity of the interim security case could be significantly weakened.

## **III. The "3+X" Defence-in-Depth Strategy: A Framework for Organisational and Procedural SecRACs**

The "3+X Justification Pillars," detailed in Section 10 of the TMF Cybersecurity Case 1, represent the primary risk management rationale for the interim commissioning phase. This strategy is particularly pertinent given that many final technical cybersecurity controls for the permanent network architecture are still pending verification and implementation. The "3+X" approach heavily emphasizes organisational and procedural measures, which align directly with the corresponding SecRAC categories from TS 50701.

### **A. Pillar 1: Total Isolation**

This pillar dictates that "Systems and components not actively undergoing commissioning or integration via the pre-production network infrastructure are maintained in a state of total isolation from this temporary infrastructure".1 This is highlighted as a critical measure, especially for safety-related assets, where the final cybersecurity controls are still under development.

* **TS50701 Alignment**: This is primarily an Organisational/Procedural SecRAC, requiring policies and procedures to enforce and verify such isolation. It can also incorporate Technical Countermeasures Outside the SuC, such as physical air gaps or administratively disconnected network segments enforced by infrastructure configurations.
* **Application in TMF**: This measure is fundamental to reducing the attack surface during the interim phase by preventing any network connectivity to systems that do not explicitly require it for ongoing commissioning tasks.

### **B. Pillar 2: Controlled Communication**

According to this pillar, "Communication pathways between connected OT systems and any external points... via the pre-production network infrastructure are strictly controlled and restricted. Access is limited to only those necessary protocols... and endpoints required for specific commissioning tasks...".1 Enforcement relies on firewall rules on interim network devices, the project's communication requirements matrix, and managed vendor access agreements, referencing DG-IT-ST031.

* **TS50701 Alignment**: This is a Combination SecRAC. It involves Technical Countermeasures (firewall rules on interim network devices) and Organisational/Procedural Countermeasures (the communication requirements matrix, access approval processes, and vendor management standards like DG-IT-ST031).
* **Application in TMF**: This pillar aims to minimize exposure by ensuring only essential and explicitly authorized data flows occur, thereby reducing potential pathways for threat propagation or unauthorized access to or from the OT systems under commission.

### **C. Pillar 3: Preventive Control Focused**

The strategy emphasizes that "The majority, if not all, of the identified countermeasures for the interim phase are preventative in nature, aiming to reduce the likelihood of security incidents occurring during commissioning".1 Examples cited include adherence to Downer's access control policies (DG-IT-ST015), change management procedures (DG-IT-ST017), close monitoring of activities by Downer personnel, reliance on documented SOPs, and physical security measures.

* **TS50701 Alignment**: This pillar primarily describes the *nature* and strategic intent of the chosen countermeasures, which are largely Organisational/Procedural SecRACs.
* **Application in TMF**: This represents a strategic choice to prioritize the prevention of security incidents, which is particularly relevant for a temporary setup that may have less mature detection and response capabilities compared to the final operational environment.

### **D. Pillar +X: Additional Defence-in-Depth Countermeasures**

Beyond the three core pillars, this component allows for the application of "additional countermeasures... following defence-in-depth principles from established frameworks such as TS 50701, IEC 62443, NIST SP-800-53, and the MITRE ATT&CK Framework".1 Specific examples for the interim phase include "heightened procedural awareness for all personnel involved in commissioning, specific contractual clauses with vendors regarding their cybersecurity responsibilities... and use of Downer-managed transient assets where possible."

* **TS50701 Alignment**: This pillar is predominantly Organisational/Procedural (heightened awareness, contractual clauses) but can also include Technical Countermeasures Outside the SuC (e.g., security features inherent in Downer-managed transient assets if they are centrally secured and managed).
* **Application in TMF**: This provides the flexibility to add further layers of security tailored to specific risks or activities encountered during commissioning, ensuring the defence-in-depth strategy can adapt.

### **E. Analysis: "3+X" as the Embodiment of Organisational/Procedural SecRACs**

The "3+X" pillars are not merely abstract guiding principles; they are actionable strategies that translate directly into tangible organisational and procedural SecRACs. For instance, achieving "Total Isolation" necessitates clear procedures for disconnecting systems, methods for verifying this isolation state, and processes for managing any exceptions. Similarly, "Controlled Communication" relies on organisational processes for defining, reviewing, and approving communication pathways, supplementing the technical enforcement by firewalls.

This "3+X" framework serves as a critical compensating strategy, particularly in light of delays or uncertainties regarding the final technical controls. The TMF Cybersecurity Case notes, "Downer has not received the final network design for all segments and will not likely receive and fully test it until just prior to, or even during, the security testing period for the final system".1 The "3+X" strategy, with its strong emphasis on achieving security through isolation and strict procedural discipline, is a direct organisational and procedural response to this reality. It represents a pragmatic acceptance of project complexities, leveraging robust procedures and organisational diligence as primary SecRACs to bridge the security gap until the comprehensive technical controls are mature and fully operational.

Furthermore, the "+X" pillar offers inherent scalability and adaptability. As new or unforeseen risks emerge during the dynamic commissioning phase, or as specific commissioning activities necessitate unique safeguards not initially envisioned, the "+X" component allows for the incorporation of additional countermeasures—be they technical, organisational, or a combination—without requiring an overhaul of the three core pillars. This makes the overall SecRAC strategy responsive and adaptable to the evolving conditions of a complex commissioning environment.

## **IV. Compensating Controls from TMF DRA as SecRAC Equivalents**

### **A. Identifying Compensating Controls in "TMF\_DRA\_Controls.pdf"**

The "TMF\_DRA\_Controls.pdf" document 1, which contains outputs from the Detailed Risk Assessment, lists numerous controls applied to various assets. Among these, certain controls are explicitly labeled as "CompensatingControl" or "Compensatingcountermeasure".1 These include:

* CompensatingControl:NISTSP800-53r5AC-17(9): Disconnect/DisableAccess, which is repeatedly associated with a wide range of assets across the facility and specialist equipment domains.1
* Compensatingcountermeasure:operatingprocedurefortrainshuntingtoincludemitigationsforspoofdigitalradiomess.1
* Compensatingcountermeasure:awarenesstrainingforstaffinvolvedintrainshuntingtoincluderiskofspoofdigitalradior.1

These are measures specifically identified during the risk assessment process to mitigate risks where standard or inherent controls within the SuC are deemed insufficient, not fully applicable, or not yet implemented. Their function is operationally identical to that of SecRACs. As defined in the context of IEC 62443, "The concept of compensating countermeasures allows a certain security level to be reached even if some requirements cannot be implemented directly".4 General cybersecurity literature also defines compensating controls as "alternative safeguards used when primary controls can't be implemented".5

### **B. Mapping DRA Compensating Controls to TS50701 SecRAC Categories**

The compensating controls identified in the TMF DRA can be mapped to the TS50701 SecRAC categories as follows:

* **NIST SP 800-53r5 AC-17(9): Disconnect/Disable Access**:
  + **Description**: This control enhancement requires organizations to possess the capability to rapidly disconnect current users who are remotely accessing an information system and/or to disable further remote access to that system.6
  + **TS50701 Alignment**: Technical Countermeasure Outside the SuC. This is a technical capability expected to be provided by the supporting network infrastructure (whether Downer corporate or the interim pre-production network) that can be invoked to protect various SuCs by severing problematic connections.
* **Procedural Mitigations for Digital Radio (Spoofing)**:
  + **Description**: These involve operatingprocedurefortrainshuntingtoincludemitigationsforspoofdigitalradiomess and awarenesstrainingforstaffinvolvedintrainshuntingtoincluderiskofspoofdigitalradior.1 These procedures and training aim to mitigate the risks of spoofed digital radio messages that could impact the safety of train shunting operations.
  + **TS50701 Alignment**: Organisational and Procedural Countermeasures. Their effectiveness relies entirely on human adherence to defined processes and the knowledge gained through training.

The presence of these compensating controls (which are functionally SecRACs) within the DRA outputs 1 indicates that the risk assessment process itself is a key driver for their definition and implementation. This aligns with cybersecurity best practices where detailed risk assessments directly inform the selection and tailoring of security controls. It also suggests that not all conditions or measures functioning as SecRACs might be explicitly labeled as such in a general security case document.1 Instead, they may be embedded within more granular risk treatment plans and control allocation tables. Therefore, a thorough review of DRA outputs is essential for a comprehensive understanding of the full SecRAC landscape employed in a project.

Furthermore, a distinction can be observed between the nature of SecRACs explicitly named in the main TMF Cybersecurity Case 1 and those identified as compensating controls in the DRA.1 The SecRACs in 1 (e.g., SecRAC-VH-001 for vendor hardening, SecRAC-RA-003 for vendor attestation) tend to be somewhat general, applying broadly to categories of interactions, particularly with vendors. In contrast, the compensating controls from the DRA (e.g., the specific operational procedures for mitigating digital radio spoofing for asset A04 1) are often highly specific, tailored to particular threats, assets, and operational contexts. This suggests a potentially two-tiered approach to SecRACs in the TMF project: broad, policy-driven SecRACs addressing common challenges of the interim phase, complemented by highly specific, risk-driven SecRACs (manifesting as compensating controls) for unique threats and vulnerabilities identified through the detailed risk assessment process.

The following table details these DRA-derived compensating controls and their SecRAC categorization:

**Table 3: Compensating Controls from TMF DRA and their SecRAC Categorization**

| **Compensating Control ID/Description** | **Associated Asset(s) or Threat(s)** | **TS50701 SecRAC Category Alignment** | **Rationale for Categorization** |
| --- | --- | --- | --- |
| CompensatingControl:NISTSP800-53r5AC-17(9): Disconnect/DisableAccess | Multiple assets across Facility and Specialist Equipment domains (e.g., A01, A04, A28, etc.) 1 | Technical (Outside SuC) | A technical capability of the supporting infrastructure to remotely terminate access, external to the SuC itself. |
| Compensatingcountermeasure:operatingprocedurefortrainshuntingtoincludemitigationsforspoofdigitalradiomess | A04: Digital Radio; Threats Fac\_T010, Fac\_T011, Fac\_T012 (Digital radio compromise) 1 | Org./Procedural | Relies on defined human actions and operational processes to mitigate risks from spoofed radio messages. |
| Compensatingcountermeasure:awarenesstrainingforstaffinvolvedintrainshuntingtoincluderiskofspoofdigitalradior | A04: Digital Radio; Threats Fac\_T010, Fac\_T011, Fac\_T012 (Digital radio compromise) 1 | Org./Procedural | Relies on enhancing human knowledge and vigilance through training to recognize and respond to potential spoofing attempts. |

## **V. Application of SecRACs and the "3+X" Framework to Key Threat Scenarios**

The practical application and interplay of explicit SecRACs, DRA-derived compensating controls, and the overarching "3+X" framework become evident when analyzing their collective effect on mitigating specific threat scenarios identified for the TMF. Appendix B of the TMF Cybersecurity Case 1 provides a comprehensive list of such threats.

### **A. Threat Scenario Example 1: Fac\_T004/T005 - Remote Exploitation or Malware Affecting BMS/HVAC Controls**

* **Threat Description**: An attacker uses a remote service (either with valid credentials obtained through illicit means or by exploiting a vulnerability) or introduces malware to tamper with Building Management System (BMS) or Heating, Ventilation, and Air Conditioning (HVAC) controls. This could result in unauthorized changes such as raising temperature setpoints or turning off critical environmental systems.1 The inherent risk for these scenarios is assessed as Medium.
* **Mitigation through SecRACs & "3+X"**:
  + **SecRAC-VH-001 (Vendor System Hardening)** 1: If the BMS/HVAC systems are vendor-supplied, this SecRAC requires vendors to perform hardening, including patching and secure configuration. This directly reduces the systems' susceptibility to remote exploitation and malware infection. This is a procedural requirement by Downer leading to a technical outcome by the vendor.
  + **SecRAC-RA-001 (JIT Access)**, **SecRAC-RA-002 (Network Isolation)**, and **SecRAC-RA-003 (Vendor Attestation)** 1: If the "remote service" involves vendor access, these SecRACs collectively limit the exposure. JIT access minimizes the time window for an attack, network isolation prevents a compromised BMS/HVAC or vendor connection from impacting the wider corporate network, and vendor attestation provides a baseline of security commitment from the vendor. These are combinations of technical and procedural/organisational measures.
  + **"3+X" Pillar - Controlled Communication** 1: This pillar, through firewall rules and defined communication matrices, restricts the protocols and endpoints accessible to and from the BMS/HVAC systems, thereby reducing potential attack vectors for remote exploitation. This is a combined technical and procedural measure.
  + **"3+X" Pillar - Total Isolation** 1: If the BMS/HVAC systems can be maintained in an isolated state when not actively being commissioned or configured, this can prevent remote access entirely, offering a strong mitigation. This is primarily an organisational/procedural measure, potentially supported by technical network disconnection.
  + **Compensating Control (NIST SP 800-53r5 AC-17(9): Disconnect/Disable Access)** 1: Should malicious activity related to remote access be detected, this technical capability (external to the SuC) allows for the rapid disconnection of the remote session, limiting further impact.

### **B. Threat Scenario Example 2: SE\_T006 - Malware Infection of Specialist Equipment Controllers via Portable Media or Transient Assets**

* **Threat Description**: Malware is introduced to specialist equipment controllers (e.g., GMAW Welding Robot, CNC Machining Centre) via infected portable media (like USB drives) or transient assets (such as vendor laptops) used during configuration or maintenance. This could lead to unexpected, large, and erratic machinery movements or system unavailability.1 The inherent risk for such scenarios is assessed as High.
* **Mitigation through SecRACs & "3+X"**:
  + **SecRAC-VH-001 (Vendor System Hardening)** 1: Hardening of the specialist equipment by the vendor might include disabling auto-run features for USB devices or implementing basic endpoint protection measures, reducing the likelihood of malware execution from portable media. This is a procedural requirement by Downer for a technical outcome by the vendor.
  + **"3+X" Pillar - (+X) Additional Defence-in-Depth Countermeasures** 1: The explicit mention of "use of Downer-managed transient assets where possible" directly addresses the risk from potentially insecure vendor laptops. This is an organisational/procedural SecRAC, potentially with technical backing if Downer's assets are centrally secured and scanned.
  + **"3+X" Pillar - Preventive Control Focused** 1: This pillar supports the implementation of SOPs for connecting any portable media or transient assets to specialist equipment. Such SOPs could mandate pre-scanning of media on a trusted terminal, or the exclusive use of Downer-issued and controlled devices. This is an organisational/procedural SecRAC.
  + **Downer Policy DG-IT-ST015 (Access Control Standard)** 1: This policy would underpin physical access controls to the specialist equipment, potentially restricting who can connect devices, and procedural controls for managing access rights to configuration interfaces. This is an organisational/procedural SecRAC.
  + **Cybersecurity Related Requirement TORCS-FAC-UC-C02 (A mobile device management plan shall be developed...)** 1: If this plan is developed and its scope extended to cover transient assets and portable media used with OT systems, it would provide a formal framework for managing these devices, functioning as an organisational/procedural SecRAC.

### **C. Threat Scenario Example 3: Fac\_T010/T011/T012 - Compromise of Digital Radio Communications Affecting Shunting Safety**

* **Threat Description**: These scenarios involve the compromise of digital radio communications, which could affect the safety of train shunting operations. Threats include physical tampering with the digital radio base station to enable external remote access for eavesdropping or sending spoof messages (Fac\_T010); an attacker using a non-facility handheld radio to spoof a legitimate user for similar malicious purposes (Fac\_T011); or a facility-owned handheld radio being lost or stolen and then used maliciously (Fac\_T012).1 The inherent risk for these is assessed as Medium.
* **Mitigation through SecRACs & "3+X"**:
  + **DRA Compensating Controls** 1: These are central to mitigating this threat:
    - Compensatingcountermeasure:operatingprocedurefortrainshuntingtoincludemitigationsforspoofdigitalradiomess: This organisational/procedural SecRAC ensures that operational staff follow specific steps designed to detect or counteract spoofed messages during safety-critical shunting.
    - Compensatingcountermeasure:awarenesstrainingforstaffinvolvedintrainshuntingtoincluderiskofspoofdigitalradior: This organisational/procedural SecRAC aims to equip staff with the knowledge to recognize potential radio interference or spoofing attempts and react appropriately.
  + **"3+X" Pillar - Preventive Control Focused** 1: This supports the development and enforcement of SOPs for the secure handling of radio equipment, including procedures for reporting lost or stolen devices promptly. This is an organisational/procedural SecRAC.
  + **Physical Security (Assumption Fac\_AS03)** 1: Robust physical security measures for the site, as assumed by Fac\_AS03, are crucial for protecting the digital radio base station from unauthorized physical access and tampering (Fac\_T010). This is an organisational/procedural SecRAC, supported by technical physical barriers.
  + **NIST SP 800-53r5 AC-18(5): Antennas and Transmission Power Levels** 1: If this control (related to managing antenna characteristics and transmission power) is applied to the digital radio system infrastructure, it could potentially limit the effective range for eavesdropping or spoofing attempts from unauthorized external devices. This would function as a Technical Countermeasure Outside the SuC.

The analysis of these threat scenarios demonstrates that effective mitigation during the TMF interim phase does not rely on a single "silver bullet" control. Instead, it hinges on the layered application of multiple SecRACs, often of different types (technical outside SuC, organisational/procedural, or combined). For instance, the threat of malware infection via portable media (SE\_T006) is addressed by a combination of vendor system hardening (a procedural demand on the vendor for a technical outcome), organisational policies regarding the use of managed transient assets, and procedural SOPs for connecting any external devices. This layering exemplifies the practical application of defence-in-depth principles through a thoughtful combination of the TS50701 SecRAC categories.

Furthermore, the criticality of SecRACs for managing threats with potential safety implications is evident. For threats like Fac\_T010-T012 (compromise of digital radio communications affecting shunting safety), the primary mitigations identified in the DRA are purely organisational and procedural SecRACs (specific operating procedures and awareness training). While the TMF Cybersecurity Case notes that Safety Integrity Level (SIL) allocation, as typically applied to railway safety interlocking functions, is not directly applicable to these TMF manufacturing/maintenance systems in the same safety-critical operational context 1, the potential for cybersecurity incidents to impact safety-related aspects of equipment operation (e.g., erratic machinery movement from threats like SE\_T001/T002, or unsafe shunting due to compromised radio) means that these organisational and procedural SecRACs assume a safety-critical role during the interim period. Their effectiveness places significant responsibility on human operators, their training, and the overall organisational discipline in adhering to these safety-enhancing procedures.

## **VI. Conclusion: Evaluating the SecRAC Approach in the TMF Interim Phase**

### **A. Summary of the Effectiveness and Necessity of the SecRAC-based Strategy**

The cybersecurity strategy for the Torbanlea Manufacturing Facility's interim commissioning phase, as documented in the "CQ20 Torbanlea Cybersecurity Case" 1, effectively leverages the concept of Security-Related Application Conditions (SecRACs) to manage identified risks. This is achieved through a combination of explicitly defined SecRACs targeting vendor interactions 1, the comprehensive "3+X" defence-in-depth framework emphasizing organisational and procedural controls 1, foundational security assumptions regarding Downer's existing environment 1, and specific compensating controls derived from the Detailed Risk Assessment (DRA).1 This multi-faceted approach is presented as a pragmatic and necessary measure to ensure an acceptable security posture for project progression during this interim phase, particularly when the final, permanent security architecture and its associated technical controls are not yet fully implemented or verified.1

### **B. The Interplay Between Technical, Organisational, and Procedural Measures**

The TMF interim cybersecurity case demonstrates a significant reliance on organisational and procedural SecRACs. These are supported by selected technical countermeasures implemented outside the direct boundaries of the Systems under Consideration (SuCs), such as interim network security features and the capability to disconnect remote access. This combination is designed to compensate for the current incompleteness of inherent technical controls within the SuCs themselves. The strength of this approach lies in its ability to provide a layered, defence-in-depth security posture. Organisational policies establish the overarching governance, procedures define expected behaviors and actions, and external technical controls provide a degree of enforcement and protection for the interim environment.

### **C. Residual Risks and Limitations of the Interim SecRAC Approach**

Despite the structured approach, the reliance on SecRACs during an interim phase inherently carries certain residual risks and limitations. A key area of concern is the dependency on vendor attestations (e.g., SecRAC-RA-003 1) and the actual diligence of vendors in hardening their systems (SecRAC-VH-001 1). The effectiveness of these SecRACs is contingent upon vendor capability, honesty, and the rigor of Downer's verification processes, reflecting broader challenges in third-party risk management.7 Similarly, the efficacy of numerous organisational and procedural SecRACs, including the "3+X" pillars, depends heavily on the consistent diligence of personnel in adhering to established procedures. Any lapses in human performance or procedural adherence can significantly weaken these controls.

The very nature of an "interim" security case implies that the current state is a temporary adaptation and not the desired final security posture. Consequently, it likely carries a higher level of inherent risk compared to the fully implemented and verified final system. Compensating controls, if not diligently managed, validated over time, and adapted to changing environments, can themselves become points of weakness or lead to a false sense of security.5

### **D. Alignment with TS50701 and Broader Cybersecurity Principles**

The TMF's SecRAC-based strategy for the interim phase, notwithstanding its temporary nature and inherent limitations, aligns with the intent of TS 50701 and the principles of related standards like IEC 62443. By formally identifying risks and addressing them through documented conditions (assumptions), external technical measures, and robust organisational/procedural countermeasures (including explicit SecRACs and DRA-derived compensating controls), the approach demonstrates a structured effort to manage cybersecurity. The TMF Cybersecurity Case concludes that "the residual cybersecurity risk for the commissioning phase is assessed by Downer as being managed to a 'Low' and acceptable level for the defined interim period".1 This assessment is predicated on the effective implementation and consistent application of the described SecRACs and supporting measures.

The SecRAC framework employed during this interim phase should not be viewed merely as a set of temporary fixes. It can serve as a valuable stepping stone towards the final, permanent security posture. Lessons learned from managing the interim phase—such as the practical effectiveness of certain vendor-related controls, challenges encountered in procedural adherence, or the utility of specific isolation techniques—can provide crucial input for refining the final security case. This ensures that the permanent controls are not only technically sound but also address real-world operational issues and human factors encountered during the commissioning process. The planned transition from the pre-production infrastructure to the final secure configuration, which will be detailed in the project's transition plans and the final Security Case report 1, should ideally incorporate these experiential learnings.

Finally, while the TMF Cybersecurity Case focuses on the interim phase, standards like TS 50701 2 and IEC 62443 advocate for cybersecurity management throughout the entire system lifecycle. SecRACs, particularly those organisational or procedural ones that prove effective and relevant beyond the interim phase, may evolve into permanent controls or inform standing operational procedures. Even if the specific interim SecRACs are superseded, as stated in the TMF document 1, the *practice* of identifying and managing security through such conditions and compensating measures is a valuable capability that may be required for future system changes, exceptions, or evolving operational contexts. This underscores the importance of embedding the principles of SecRAC management into the broader cybersecurity governance framework.

#### Works cited

1. TMF Cybersecurity Case -JTMv2.pdf
2. CLC/TS 50701:2023 - Railway applications - Cybersecurity - iTeh Standards, accessed June 10, 2025, <https://standards.iteh.ai/catalog/standards/clc/db257ea9-8ba0-4f4c-a791-df34a6030541/clc-ts-50701-2023>
3. CLC/TS 50701:2021 - Railway applications - Cybersecurity - iTeh Standards, accessed June 10, 2025, <https://standards.iteh.ai/catalog/standards/clc/1a4316e5-3b11-4d71-b561-a7978b8f408c/clc-ts-50701-2021>
4. IEC 62443 - SyC Smart Energy, accessed June 10, 2025, <https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/>
5. The Ultimate Guide to Compensating Controls - Metricstream, accessed June 10, 2025, <https://www.metricstream.com/learn/compensating-controls.html>
6. 800-53|AC-17(9) | Tenable®, accessed June 10, 2025, <https://www.tenable.com/audits/references/800-53/AC-17(9)>
7. 6 Types of Vendor Risks and Loss (2025 Guide) - Safe Security, accessed June 10, 2025, <https://safe.security/resources/blog/6-types-of-vendor-risks-you-should-monitor/>
8. A Call to Do Better at Vendor Security Risks - NAVEX, accessed June 10, 2025, <https://www.navex.com/en-us/blog/article/a-call-to-do-better-at-vendor-security-risks/>
9. Third-Party Security Risk Management: 7 Best Practices - Syteca, accessed June 10, 2025, <https://www.syteca.com/en/blog/third-party-providers>
10. Compensating Controls: The Unsung Heroes of Cyber Resilience - Reach Security, accessed June 10, 2025, <https://www.reach.security/blog/compensating-controls-the-unsung-heroes-of-cyber-resilience>
11. Rail Cybersecurity Compliance & Regulations - Cervello.Security, accessed June 10, 2025, <https://cervello.security/compliance/>