Set of ACR development guidelines

Towards an Autonomous Cyber Resilience Engineering Framework

TNO Public ⟩ TNO 2025 P12764
8 August 2025

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 P12764 – 8 August 2025

Set of ACR development guidelines

Towards an Autonomous Cyber Resilience Engineering Framework

Author(s)	Ali, M. (Mahira) Fransen, F. (Frank)
Classification report	TNO Public
Title	TNO Public
Report text	TNO Public
Appendices	TNO Public
Number of pages	33 (excl. front and back cover)
Number of appendices	2

All rights reserved
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

© 2025 TNO

Contents

Appendices

1 Introduction

Cybersecurity has undeniably strengthened over the years [1]. Organisations have invested heavily in technologies, frameworks, and protocols to protect their digital assets. However, this progress has not gone unnoticed by adversaries. Attackers have evolved in parallel, developing increasingly sophisticated techniques that challenge even the most advanced defences.

This dynamic has created a continuous cyber rat race. On the defence side, maintaining security consumes ever-growing amounts of manpower, financial resources, and technical infrastructure [2]. Despite the abundance of security tools, platforms, and educational materials, a persistent lack of awareness among users and stakeholders remains a critical vulnerability [3]. Human error, negligence, and insufficient understanding of basic security hygiene continue to undermine even the most robust systems.

Compounding this issue is the increasing complexity of digital infrastructures. Organisations now operate in hybrid environments with cloud-native systems, legacy components, and third-party integrations. On top of this complexity, they must navigate a dense landscape of cybersecurity legislation, surplus of countermeasures, and cope with a global shortage of skilled professionals.

1.1 Need for Autonomous Cyber Resilience

The challenges — technical complexity, regulatory pressure, limited expertise, and low awareness — make it clear that traditional approaches to cybersecurity are no longer sufficient. Given the scale and intricacy of modern infrastructures, it is no longer feasible to manually oversee every component or respond to every threat in real time with human operated security. Moreover, cyberattacks are getting more automated and use artificial intelligence (AI), enabling these attacks to take place at machine speed, whereas the response is still mostly at human speed. This all necessitates the adoption of autonomous capabilities. Furthermore, it became evident that perfect security is unattainable — not only due to the evolving threat landscape but also because human factors consistently introduce weaknesses — making resilience essential. Hence, this calls for a paradigm shift: from reactive defence to proactive security. This necessitates a focus on Autonomous Cyber Resilience (ACR), defined in accordance with [4] as:

> ‘ *the ability of a (digital computing) system to*
> *anticipate, withstand, recover from, and adapt to*
> *cyberattacks and unintended disruptions*
> *to ensure mission or business objectives*
> *without being controlled directly by humans.* ’

While the broader system does not need to be fully autonomous, ACR can be conceptualised as an autonomous subsystem embedded within (see Figure 1.1). This subsystem is comprised of components that enable the system to autonomously anticipate, withstand, recover from, and adapt to cyber threats. Where autonomously means among others without requiring direct human control and being able to respond and adapt in real time. These components may include monitoring agents, adaptive response mechanisms, and learning modules, often structured around the MAPE-K loop (Monitor, Analyse, Plan, Execute over a shared Knowledge) [5].

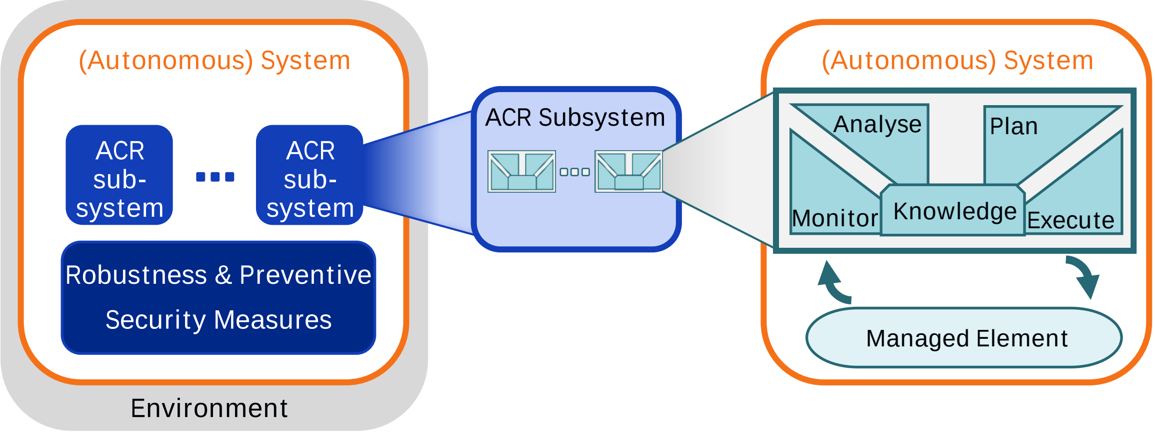


Figure 1.1: Conceptual placement of ACR as an autonomous subsystem within an (autonomous) system.

However, achieving ACR requires more than just these dynamic elements. It also depends on a broader set of enablers: robustness techniques (e.g., fault-tolerant design, redundancy) and preventative security measures (e.g., access control, encryption). While these enablers are not part of the ACR subsystem per se, they are essential to its effectiveness and must be considered in the system's overall design.

1.2 Cyber Resilience Engineering

Developing cyber resilient systems is not a trivial task. To support systems engineering with this task, several approaches have been developed that provide guidance on how to apply cyber resiliency concepts, techniques (i.e., building blocks) and engineering practices during the systems engineering process. Over the years, different, typically academic, approaches for designing and developing cyber resilient systems have been proposed. These are often domain specific, such as military, telecom, and cyber-physical systems. The most mature is the Cyber Resiliency Engineering Framework (CREF) developed by The MITRE Corporation, that has been standardised in NIST SP 800-160 Volume 2 [6], and is described in Subsection 1.2.1.

Given the extensive body of research on robustness and resilience within the domain of network and telecom, it is worthwhile to highlight ongoing developments in this field. For example, the EU COST action 'Resilient Communication Services Protecting End-user Applications from Disaster-based Failures' (RECODIS) brought researchers from all over Europe together to work on the topic. An overview of the work is collected in [7]. A systematic approach to the engineering of network resilience was introduced in [8] that consists of a control loop comprising a number of conceptual components that realise the real-time aspect of the D2R2 + DR strategy, and consequently implement network resilience. The D2R2 + DR stands for Defend, Detect, Remediate, Recover, and Diagnose and Refine, and was introduced in [9].

In recent years, the definition, design and specification of 6G mobile communications systems has started. The International Telecommunication Union (ITU) has identified resilience as key factor in the design, deployment, and operational consideration of 6G systems [10]. In addition, in the beginning of 2024 several countries released a *Joint*

Statement Endorsing Principles for 6G: Secure, Open, and Resilient by Design[1]. Several academic papers have now been published on resilient-by-design methodologies for 6G, [11], [12], and [13]. Since 6G has a strong focus on use of AI and zero-touch networking, the authors of the papers implicitly assume the resilience capabilities to be (semi-)autonomous.

A whole different approach is security chaos engineering, a method to automatically subject a system to (chaotic) input and failures to test and increase its resilience as described in [14]. Although this is not a guidance framework for how to design and develop cyber resilient systems, it does provide a different perspective on the nature of cyber resilience.

1.2.1 MITRE Cyber Resilience Engineering Framework

MITRE Cyber Resilience Engineering Framework (CREF) (see Figure 1.2) provides structured guidance for embedding cyber resilience into systems, in alignment with NIST SP 800-160 Volume 2 [6]. The framework is structured into four components: *cyber resiliency goals*, *objectives*, *techniques* and *approaches*. The *goals* — built on the four pillars, namely, *Adapt*, *Anticipate*, *Recover*, and *Withstand* — provide linkage between risk management decisions at system level.

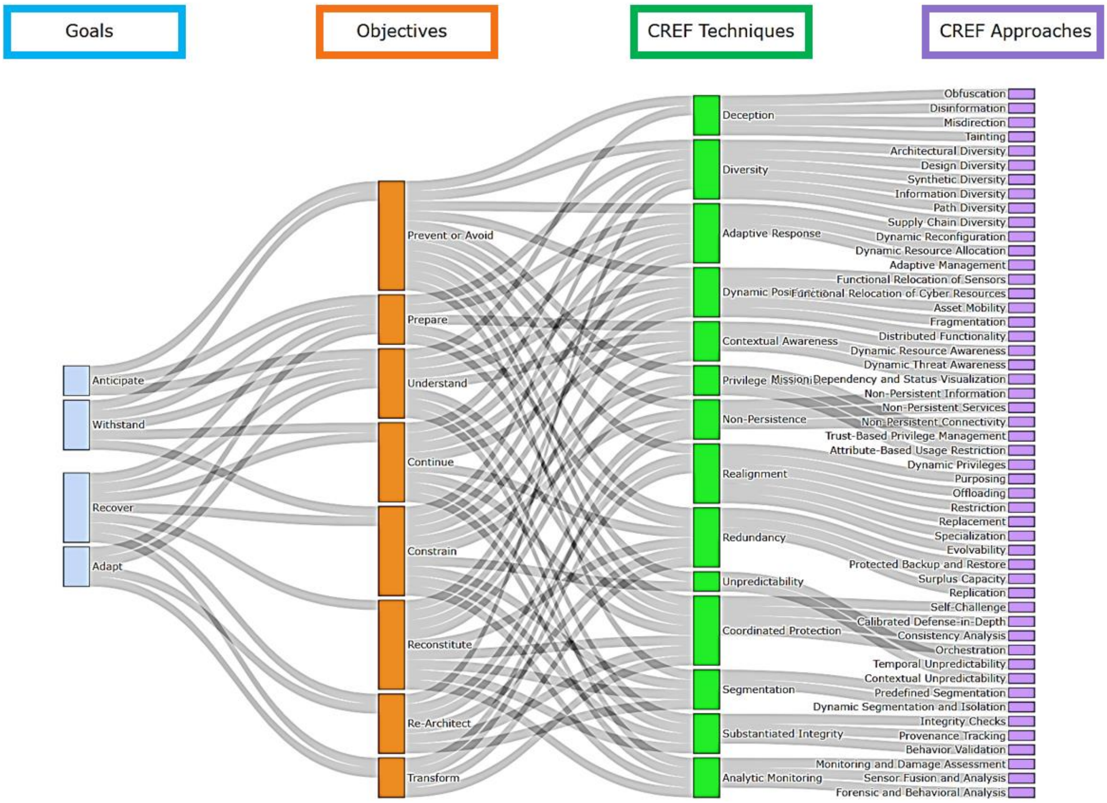


Figure 1.2: MITRE Cyber Resilience Engineering Framework (CREF) Navigator [15].

These *goals* are further refined into *objectives*, which define what the system is intended to achieve within its operational environment. This allows stakeholders to prioritise resilience

[1] https://www.ntia.gov/speechtestimony/2024/joint-statement-endorsing-principles-6g-secure-open-resilient-design,

based on organisational missions or business functions. Together, the *cyber resiliency goals* and *objectives* form a vocabulary for describing what properties and capabilities are needed.

In contrast, *cyber resiliency techniques* and *approaches* provide a vocabulary for how a system can realise these *cyber resiliency goals* and *objectives*. A *technique* comprises a set of interdependent practices and technologies designed to achieve one or more goals or objectives by providing capabilities. For each *technique*, multiple non-exhaustive representative *approaches* are identified to implement the *technique*.

In order for a system to embed resilience as defined by CREF, the system as a whole must adhere to its principles — not only at the system level but also within its internal ACR subsystems. This implies that each ACR subsystem must itself be resilient, as the system's overall resilience is contingent on the resilience of its constituent parts.

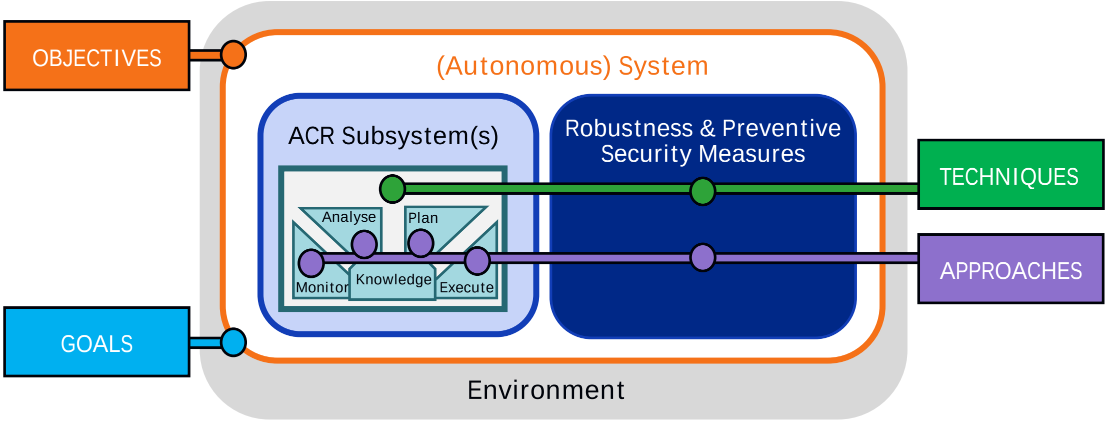


Figure 1.3: Layered system-level overview showing the conceptual placement of MITRE CREF elements.

In context of embedding cyber resilience into autonomous systems, CREF elements can be conceptually positioned across the system layers (see Figure 1.3). *Goals* and *objectives* operate at the interface between the system and its environment: *goals* define high-level resilience priorities aligned with mission needs, while *objectives* translate these into system-specific expectations that guide ACR subsystem design. *Techniques* describe the resilience capabilities required to meet these *objectives* and can be mapped to combinations of MAPE functions within the ACR subsystem. *Approaches*, in turn, represent specific implementations of these techniques, corresponding to individual MAPE elements.

1.2.2 Autonomous Cyber Resilience Engineering Framework

The Autonomous Cyber Resilience Engineering Framework (A-CREF), proposed in Section 3, builds upon the foundational principles of the MITRE CREF, adapting its structure to support the autonomous implementation of resilience strategies. While A-CREF shares the overarching goal of NIST SP 800-160 [6] — namely, to guide the development of trustworthy, resilient systems — it extends this objective by explicitly incorporating autonomy. In doing so, A-CREF aims to address resilience challenges across the entire system lifecycle, with a focus on reducing human dependency and enabling self-directed, adaptive behaviour.

For this purpose, A-CREF redefines traditional resilience components by enabling them to function autonomously — referred to as dynamic ACR elements — while preserving the robustness and preventative measures that underpin resilient system design. By formalising this autonomous subset, the framework supports the design of systems that are not only resilience-oriented but also capable of achieving resilience with minimal human intervention. This shift facilitates the development of scalable, self-sustaining security architectures that are better aligned with the demands of modern, complex operational environments.

1.3 Document Guide

This document introduces the first version of ‘the Autonomous-Criteria’, a formalised set of capabilities required for a system’s component to be considered autonomous. Here, the contribution and outline of the document are defined.

1.3.1 Contribution

This document is Deliverable D.1 of TNO’s Early Research Programme ’Cyber-Secure Systems by Design’, within Research Line 2 ‘Autonomous Cyber Resilient Operations’. The goal of this document is to deliver a first version of ’the Autonomy Criteria ’. These criteria are intended to evaluate the components of the MITRE Cyber Resilience Engineering Framework (CREF) in terms of their potential for autonomous enablement. This assessment serves as the foundation for developing the Autonomous Cyber Resilience Engineering Framework (A-CREF) — a structured approach to identifying and guiding the integration of autonomy into cyber resilience practices.

1.3.2 Outline

This document follows a structured methodology that combines a literature analysis to validate through real-world systems and framework application. The content is organised as follows:

- Chapter Error! Reference source not found. starts with a literature-based derivation of the *Autonomy Criteria* . This phase identifies foundational capabilities of autonomy in systems and formulates a structured set of criteria. These criteria are then validated against a selection of real-world autonomous systems, identified through a literature study. The validation assesses whether systems claiming autonomy exhibit the capabilities defined by the *Autonomy Criteria* .

- Chapter 3 applies the validated criteria to selected techniques and approaches within the MITRE CREF. This analysis determines which CREF components can be autonomously realised and what capabilities are required for such transformation. This step lays the groundwork for the development of A-CREF.

- Chapter 4 outlines refinements of A-CREF and proposes research directions to advance the formalisation of *autonomous resilient systems by design*.

This integrated structure ensures that the development of A-CREF is both theoretically grounded and practically validated, offering a robust pathway towards autonomous cyber resilience system engineering by design.

2 Autonomy Criteria

This chapter develops criteria — referred to as the *Autonomy Criteria* — used to define the foundational capabilities that allow a system to function autonomously. In Section 2.1, this criteria is initially derived from well-established definitions of autonomy. These sources provide a conceptual basis for identifying the core capabilities that characterise autonomous systems. To validate this criteria, a literature review was conducted in Section 2.2, focusing on real-world systems that claim to exhibit autonomous behaviour, while also highlighting instances where claims of autonomy may be overstated or inconsistently applied in practice. This two-step approach ensures that the criteria are both theoretically grounded and empirically supported, enhancing their relevance and applicability to the evaluation of CREF components.

2.1 Autonomy Criteria Establishment

The absence of a universally accepted definition of what constitutes an autonomous system is evident [16]. In response to the growing adoption of *autonomous capabilities* in military systems, NATO published a report series in 2015 [17]. Herein, they address the challenges associated with autonomous systems — among them, the persistent lack of clarity concerning what autonomy entails within systems. Based on their findings, NATO defines an autonomous system as a system that is [17]:

> ‘ *capable of understanding higher-level intent and direction.*
> *From this understanding and its perception of its environment,*
> *such a system can take appropriate action to bring about a desired state.*
> *It is capable of deciding a course of action, from a number of alternatives, without*
> *depending on human oversight and control, although these may still be present.* ‘

While such definitions offer a useful starting point, they often remain abstract and open to interpretation. Therefore, to meaningfully assess whether a system can function autonomously, it is necessary to translate this conceptual definition into practical, evaluable criteria. This section proposes such a framework — the *Autonomy Criteria* — consisting of two parts: preconditions (Subsection 2.1.1) which determine whether the concept of autonomy is relevant to a given system, and capabilities (Subsection 2.1.2) which specify the functional abilities a system must demonstrate to be considered autonomous.

2.1.1 Preconditions

Prior to assessing whether a system can be altered to function autonomously, it is essential to determine whether the concept of autonomy is relevant in the system’s operational context. Autonomy may not be meaningful or necessary in every system; therefore the relevance must be established prior to applying the *Autonomy Criteria* . To support this, two preconditions are proposed to evaluate the appropriateness of considering autonomy for a given system (component), namely the presence of **dynamic behaviour** and **environmental variability** [18].

Implementing autonomy in systems that do not require dynamic behaviour — where operations are not impacted by changes in internal or external conditions — offers limited practical benefit. Autonomy is fundamentally intended to enable adaptive decision-making in response to varying conditions. When a system operates in a static manner without the need for situational responsiveness, the added complexity and resource demands of autonomy are unjustified.

Furthermore, deploying autonomy in fully predictable and stable environments lacks merit. Autonomy proves valuable in contexts where environmental uncertainty or variability necessitate real-time adaptation and decision-making. In contrast, static environments — where inputs and outcomes are known in advance — are better served by rule-based automation or scripted logic. Introducing autonomy in such settings increases system complexity without delivering proportional gains in performance or flexibility.

In the absence of variability and within static, predictable environments, autonomy becomes redundant. Introducing autonomous capabilities in such settings adds unnecessary complexity, at the expense of system transparency and maintainability — especially when simpler solutions would suffice [19]. Moreover, it diverts valuable resources that could be more effectively used elsewhere. Therefore, careful assessment of the environment and system requirements should precede any decision to implement autonomy. These preconditions serve as preliminary filters, ensuring that autonomy is only considered in contexts where it is functionally and operationally relevant.

2.1.2 Capabilities

Song et al. [20] conducted an exploratory study combining insights from literature and practitioners to conceptualise autonomous systems. Despite again the lack of a universal definition, Song et al.'s framework and NATO's findings show convergence on four fundamental capabilities that characterise a system autonomous. Specifically, an autonomous system is generally expected to be capable of carrying out — without human intervention — the capabilities identified in Table 2.1. To enhance conceptual clarity and ensure alignment with established engineering frameworks, these four autonomous capabilities have been mapped to the MAPE-K loop.

Table 2.1: The four capabilities that are required for a system to function autonomously.

Capability	MAPE-K Component	Definition
Awareness	Monitor + Knowledge	The system continuously perceives and interprets internal states and external environmental conditions, maintaining a contextual model of its operational domain.
Decision Making	Analyse + Plan	The system evaluates multiple courses of action based on its goals, current state, and environmental inputs, selecting the most appropriate strategy.
Adaption	Whole control loop	The system modifies its behaviour over time by learning from outcomes and adjusting its strategies to improve performance.
Actuation	Execute	The system carries out selected actions autonomously to achieve its goals, interfacing with physical or digital components as needed.

2.2 Literature study

To identify relevant literature, a structured approach based on the principles of Systematic Literature Review (SLR) has been developed. This methodology ensures transparency, repeatability, and comprehensiveness in the selection and analysis of sources. To enhance efficiency and scalability, artificial intelligence (AI) has been integrated into several stages of the process.

An overview of the SLR-based approach is presented in Figure 2.1. In this figure, the dashed orange boxes indicate the specific steps where AI tools were employed. The approach is divided into three sequential stages: search, screen, and analyse.

In the search stage (**Subsection** 2.2.1), relevant keywords and information sources are identified. These form the basis for constructing a targeted search query aimed at retrieving a broad, yet relevant, set of publications.

The screening stage (**Subsection** 2.2.2) involves the application of predefined inclusion and exclusion criteria to filter the initial set of results, ensuring that only the most relevant and accessible publications were retained. To structure the screening process, the open-source machine learning tool ASReview[2] was employed. ASReview facilitates title and abstract screening through an active learning approach, wherein users manually label the relevance of records. The system continuously updates its ranking based on these inputs to prioritise potentially relevant studies. Additionally, the platform allows users to tag and annotate documents during the screening process. Although ASReview supports the use of stopping heuristics — such as ceasing screening after encountering a specified number of consecutive irrelevant records — no such heuristic was applied in this case.

In the analysing stage (**Subsection** 2.2.3), a review prompt was developed. This serves as a structured prompt for a large language model (LLM) — in this case, Microsoft CoPilot[3] — to extract key elements from the selected literature. The resulting content was then used as validation input for the identified foundational capabilities of autonomous system.

2.2.1 Search

Figure 2.2 provides a schematic overview of the selected keywords and their construction. To identify relevant keywords for the literature study, the initial focus was placed on ensuring that the selected publications explicitly addressed systems. As such, a primary inclusion criterion was that the abstract must contain the term *system*. This requirement was intended to filter out literature that centred on peripheral elements such as applications, datasets, or services.

Furthermore, emphasis was placed on selecting literature that discusses deployed systems rather than purely conceptual or theoretical models. This decision was made to ensure that the extracted capabilities reflect practical, real-world implementations of autonomy, thereby enhancing the relevance and applicability of the resulting *Autonomy Criteria* .

[2] Smarter Systematic Reviews with Open-Source AI | ASReview
[3] Microsoft CoPilot

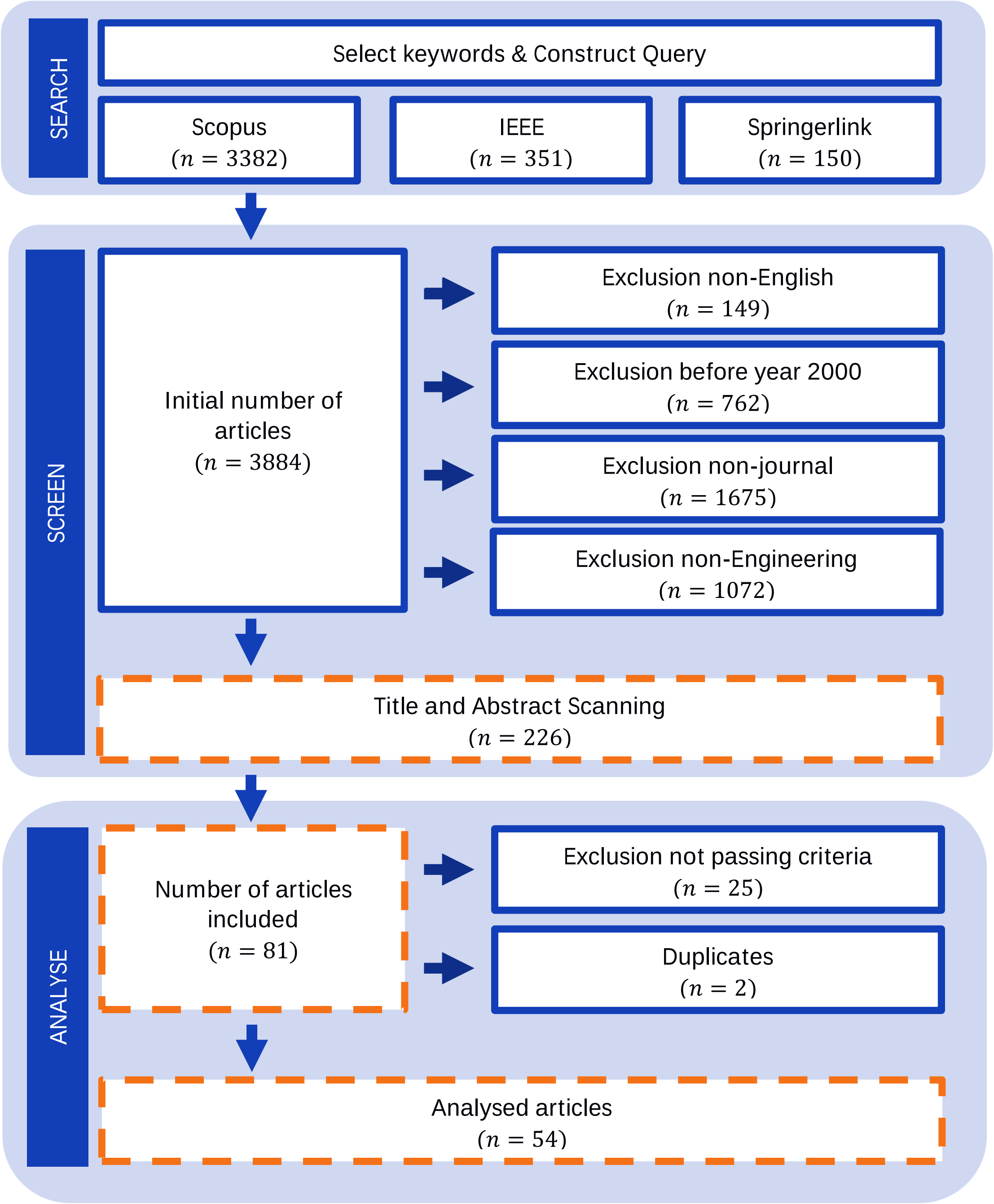

SEARCH
Select keywords & Construct Query
Scopus $(n = 3382)$
IEEE $(n = 351)$
Springerlink $(n = 150)$
SCREEN
Initial number of articles $(n = 3884)$
Exclusion non-English $(n = 149)$
Exclusion before year 2000 $(n = 762)$
Exclusion non-journal $(n = 1675)$
Exclusion non-Engineering $(n = 1072)$
Title and Abstract Scanning $(n = 226)$
ANALYSE
Number of articles included $(n = 81)$
Exclusion not passing criteria $(n = 25)$
Duplicates $(n = 2)$
Analysed articles $(n = 54)$

Figure 2.1: Overview of the used SLR-primary based approach to identify relevant literature in order to set up the *Autonomy Criteria* . Here, the orange dashed boxes are steps with AI involvement.

To ensure the literature specifically addresses autonomous systems, the search strategy was refined to target publications that explicitly combine the terms *autonomous*, *automated*, or *unmanned* with *system*. This adjustment strengthens the focus on systems where autonomy is not merely conceptual but is operationalised through concrete technological mechanisms. While ideally such criteria would be applied independently of the term *system* to capture a broader spectrum of automation-enabling technologies (e.g., artificial intelligence, machine learning, self-* capabilities), the current approach prioritises precision to maintain a clear and consistent scope.

Hence, the keyword search query was as follows:

```
ABS( “autonomous system” OR “automated system” OR “unmanned system”) AND
NOT TITLE-ABS-KEY ( algorithm OR method OR methodology OR approach OR model
OR technique OR "theor*" OR conceptual OR strategy OR framework OR review
OR survey OR application OR service OR software OR tool OR program OR
dataset OR database OR function OR chatbot OR simulation )
```

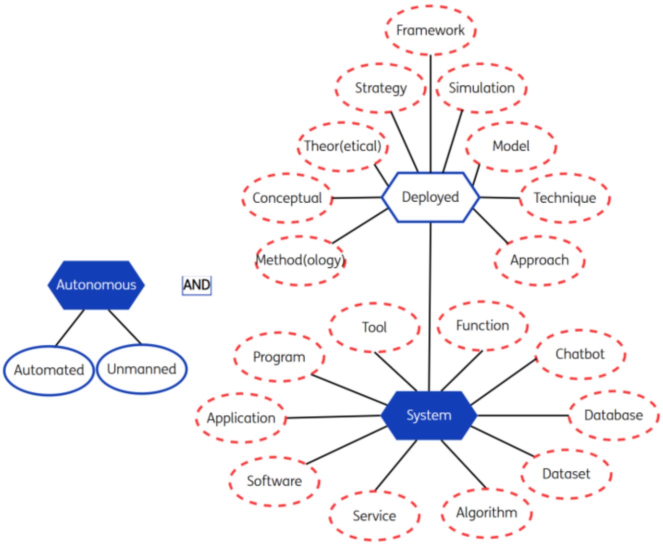


Figure 2.2: A schematic overview of the selected keywords, their construction and inclusion / exclusion. Primary keywords, represented by hexagons, serve as the basis for identifying related terms, shown as ovals. Blue solid lines indicate terms that were included in the search strategy, while red dotted lines denote those that were explicitly excluded.

The databases Scopus, IEEE Xplore, and SpringerLink were selected for the literature search due to their broad coverage of relevant fields as well as their technical compatibility with ASReview through CSV export functionality. These platforms also support advanced querying, allowing for precise and replicable search strategies. While other databases such as Elsevier ScienceDirect or ACM Digital Library may also contain relevant material, they were excluded due to limited export options or incompatible interfaces. This may have excluded potentially relevant literature; however, the selected databases are considered sufficiently comprehensive for the scope and objectives of this study. The exact search queries used for each database are provided in Appendix A.

2.2.2 Screen

Prior to screening titles and abstracts, an initial set of inclusion / exclusion criteria was applied to the results returned by the search query. This preliminary filtering step was undertaken to ensure that only high-quality, relevant, and contextually appropriate literature was considered in the subsequent analysis. The following categories of results were excluded from screening:

- **Non-English Publications:** Only papers written in English were included. This restriction is justified by the need to ensure accurate interpretation and consistent analysis of the literature. While valuable research is published in many languages, the vast majority of high-impact academic work is published in English. Additionally, limitations in translation resources could introduce interpretation bias or reduce analytical depth.

- **Publications prior to 2000:** Only papers published from the year 2000 onward were considered. This cut-off was selected to ensure the relevance of the technological context. Autonomous systems have evolved significantly in the past two decades, and earlier works often reflect outdated assumptions, limited computing capabilities, or technological constraints that no longer apply. By focusing on post-2000 literature, the analysis remains grounded in contemporary concepts, challenges, and system architectures.

- **Non-Journal Publications:** Only peer-reviewed journal articles were included. This decision is based on the nature of journal publications, which generally represent more mature research. Journal articles typically undergo a more extensive peer-review process than conference papers, often involving multiple rounds of review, critical feedback, and substantial revisions. As such, they tend to provide more in-depth theoretical grounding, comprehensive evaluations, and broader contextualisation of results. Given the objective of developing well-founded and stable criteria for autonomy, journal publications offer a more reliable and authoritative knowledge base. While conference papers are valuable for highlighting emerging ideas, their often-preliminary nature makes them less suitable as a foundation for long-term conceptual frameworks.

- **Non-Engineering Field:** Only papers situated within the field of engineering were considered. This restriction is justified by the substantial variation in how the concept of autonomy is defined across disciplines. For example, in fields such as biology, psychology, or philosophy, autonomy often refers to self-regulation, moral agency, or personal independence — definitions that differ fundamentally from the system-level autonomy considered in this study. To maintain conceptual clarity and ensure relevance to the technical domain of autonomous systems, the focus is limited to definitions and frameworks grounded in engineering.

The titles and abstracts of the remaining results were screened using ASReview. No stopping heuristic or sampling strategy was applied. Instead, the full set of results was manually screened. During this process, each paper was evaluated to determine whether the system discussed was a real-world or deployable system, and whether it claimed to incorporate specific functionalities or design principles intended to enable or enhance system autonomy.

2.2.3 Analyse

The screened results were analysed using the LLM CoPilot through the application of a structured review prompt, which is detailed in Appendix B. This prompt consists of two main components: a general section and a content-specific section. The general section is designed to extract basic metadata from the article, such as the title and author(s), to verify that the LLM has correctly identified the intended document. Following this verification, the article is subjected to a relevance assessment. This assessment evaluates whether the paper (1) discusses a deployed system, (2) introduces functionalities that enable autonomy within that system, and (3) treats these functionalities as a central element of the paper's contribution. If all three criteria are met, the article qualifies for further in-depth analysis.

For the in-depth analysis, the LLM was tasked with identifying the components introduced by the system to enable or enhance autonomy. It extracted the specific functionalities these components contribute and attempted to map them to four predefined capabilities: Awareness, Decision-Making, Adaptation, and Actuation. This automated mapping served as a preliminary classification. Subsequently, a manual review of each article was conducted to verify the identified components and functionalities. During this review, the initial mappings were critically assessed and revised where necessary. To facilitate cross-domain comparison, the extracted functionalities were further abstracted into generalised capabilities. The consolidated results of this analysis are presented in Figure 2.4.

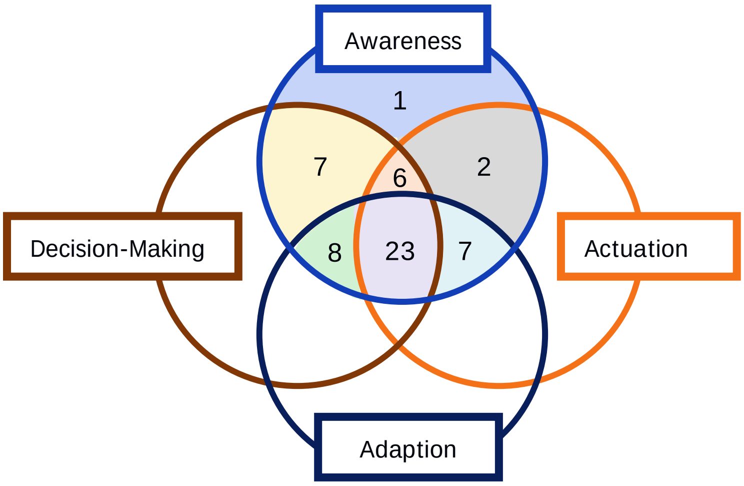


Figure 2.3: Venn diagram showcasing how the four capabilities — Awareness, Decision-Making, Adaption and Actuation — are distributed across the 54 analysed systems in the literature study.

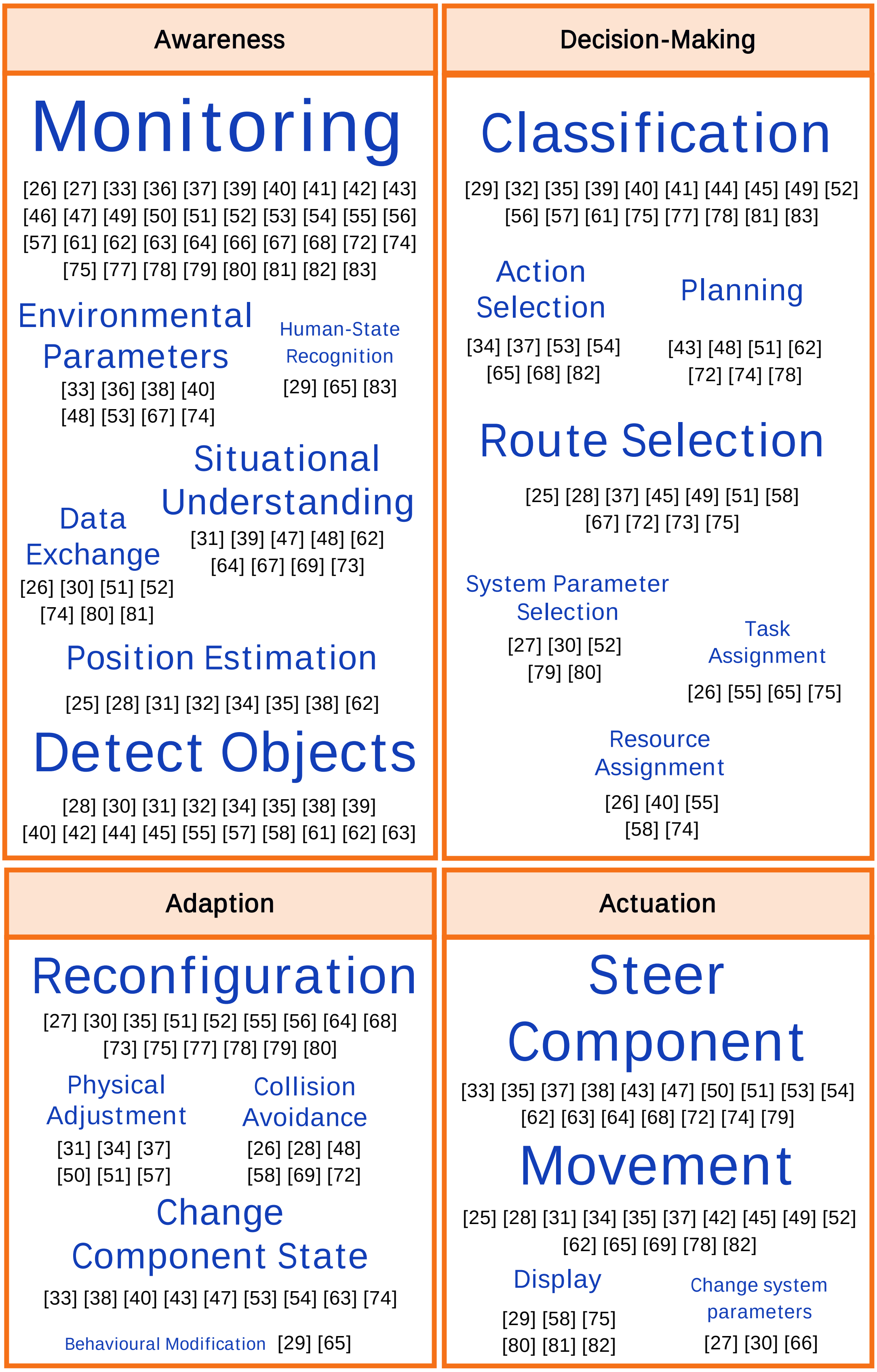
As illustrated in Figure 2.3, while all systems exhibit a certain form of *Awareness*, only 46% demonstrate all four identified capabilities. This indicates that the claim of autonomy is not self-evidently associated with the other three capabilities. The remaining 54% lack one or more capabilities, suggesting that claims of autonomy may be either overstated or narrowly defined.

For instance, systems lacking *Adaption* were found in high-precision or safety-critical domains, such as self-driving vehicles, assistive robots and healthcare technologies. This absence reflects the ongoing concern that dynamic learning mechanisms may introduce unacceptable risks in these contexts. Although such systems may operate autonomously within tightly controlled environments, their rigidity constrains broader applicability.

Similarly, systems without *Decision-Making* capabilities typically function as supportive tools. These systems assist or enhance human-led decisions but do not independently select actions, thereby falling short of full autonomy. Examples include detectors and resource optimisation tools.

Notably, in systems tasked with physical operations — such as parking or assembly — *Actuation* capabilities were often missing. These systems exhibited cognitive competence but remained operationally passive, relying on external components to execute decisions. This raises questions about the completeness of their autonomy. Likewise, systems that possess only Awareness and Decision-Making are limited to interpretation and reasoning, without the ability to adapt or act. Such systems are better classified as decision-support tools rather than autonomous agents.

Hence, this analysis underscores the necessity of all four capabilities for a system to be considered fully autonomous. Each capability contributes a distinct and essential function. In the absence of any one, a system may still be intelligent or useful, but it cannot be regarded as fully autonomous. This framework not only delineates the boundaries of autonomy but also offers a structured basis for evaluating future systems and their claims.



Awareness

Monitoring
[26] [27] [33] [36] [37] [39] [40] [41] [42] [43] [46] [47] [49] [50] [51] [52] [53] [54] [55] [56] [57] [61] [62] [63] [64] [66] [67] [68] [72] [74] [75] [77] [78] [79] [80] [81] [82] [83]

Environmental Parameters
[33] [36] [38] [40] [48] [53] [67] [74]

Human-State Recognition
[29] [65] [83]

Situational Understanding
[31] [39] [47] [48] [62] [64] [67] [69] [73]

Data Exchange
[26] [30] [51] [52] [74] [80] [81]

Position Estimation
[25] [28] [31] [32] [34] [35] [38] [62]

Detect Objects
[28] [30] [31] [32] [34] [35] [38] [39] [40] [42] [44] [45] [55] [57] [58] [61] [62] [63]

Decision-Making

Classification
[29] [32] [35] [39] [40] [41] [44] [45] [49] [52] [56] [57] [61] [75] [77] [78] [81] [83]

Action Selection
[34] [37] [53] [54] [65] [68] [82]

Planning
[43] [48] [51] [62] [72] [74] [78]

Route Selection
[25] [28] [37] [45] [49] [51] [58] [67] [72] [73] [75]

System Parameter Selection
[27] [30] [52] [79] [80]

Task Assignment
[26] [55] [65] [75]

Resource Assignment
[26] [40] [55] [58] [74]

Adaption

Reconfiguration
[27] [30] [35] [51] [52] [55] [56] [64] [68] [73] [75] [77] [78] [79] [80]

Physical Adjustment
[31] [34] [37] [50] [51] [57]

Collision Avoidance
[26] [28] [48] [58] [69] [72]

Change Component State
[33] [38] [40] [43] [47] [53] [54] [63] [74]

Behavioural Modification [29] [65]

Actuation

Steer Component
[33] [35] [37] [38] [43] [47] [50] [51] [53] [54] [62] [63] [64] [68] [72] [74] [79]

Movement
[25] [28] [31] [34] [35] [37] [42] [45] [49] [52] [62] [65] [69] [78] [82]

Display
[29] [58] [75] [80] [81] [82]

Change system parameters
[27] [30] [66]

Figure 2.4: Word cloud visualisation of generalised functionalities — found in the analysed literature — categorised under the four identified capabilities: Awareness, Decision-Making, Adaption and Actuation.

3 A-CREF

This chapter outlines the steps taken towards the development of A-CREF — a framework designed to support the engineering of systems that are resilient by design and capable of achieving this resilience autonomously. Section 3.1 outlines the first step towards the construction of A-CREF. Then, Section 3.2 applies this step.

3.1 Establishing the basis for A-CREF

To initiate the development of the A-CREF, the CREF components are redefined in terms of the identified autonomous capabilities. As discussed in Subsection 1.2.1, this redefinition is intentionally not applied at the level of goals and objectives. These high-level components, while essential for strategic alignment, do not encapsulate functional implementation details. Autonomous capabilities, by contrast, are inherently tied to implementation-level constructs. This mismatch in abstraction levels justifies excluding goals and objectives from direct mapping to the *Autonomy Criteria* .

Instead, the focus is on the technique and approach levels within CREF. While the approach level often reflects partial implementations or combinations of MAPE-K functions, it lacks the granularity and completeness required to assess autonomy effectively. Autonomy in cyber resilience is not merely about the presence of individual MAPE components, but about the orchestration of these components into coherent, self-governing functions.

Therefore, the technique level is the most appropriate component for applying the complete *Autonomy Criteria* . Techniques typically represent fully specified functions that can independently be evaluated for their capacity to operate autonomously. By assessing autonomy at the technique level, actionable insights are gained into which functions require augmentation — such as awareness, decision-making, or adaptive execution — to become truly autonomous.

While the *Autonomy Criteria* includes preconditions, these are primarily relevant when assessing whether it is meaningful or feasible to make a system autonomous. However, in the context of applying the autonomy criteria at the technique level, such preconditions can be reasonably omitted. This is because techniques are abstracted from specific deployment contexts and are evaluated primarily on their functional completeness and autonomy-enabling characteristics.

3.2 Criteria applied to MITRE CREF Techniques

To illustrate how autonomy can be integrated within the CREF techniques, the conceptual model of the ‘autonomy technique’ is introduced. Figure 3.4 depicts the generic *autonomy technique* for each CREF technique, derived by applying the *Autonomy Criteria* . As established in Subsection 2.1.2, the capabilities align with the MAPE-K loop, providing a structured lens through which the interaction of autonomous capabilities can be understood. This alignment supports the positioning of each capability within the conceptual model.

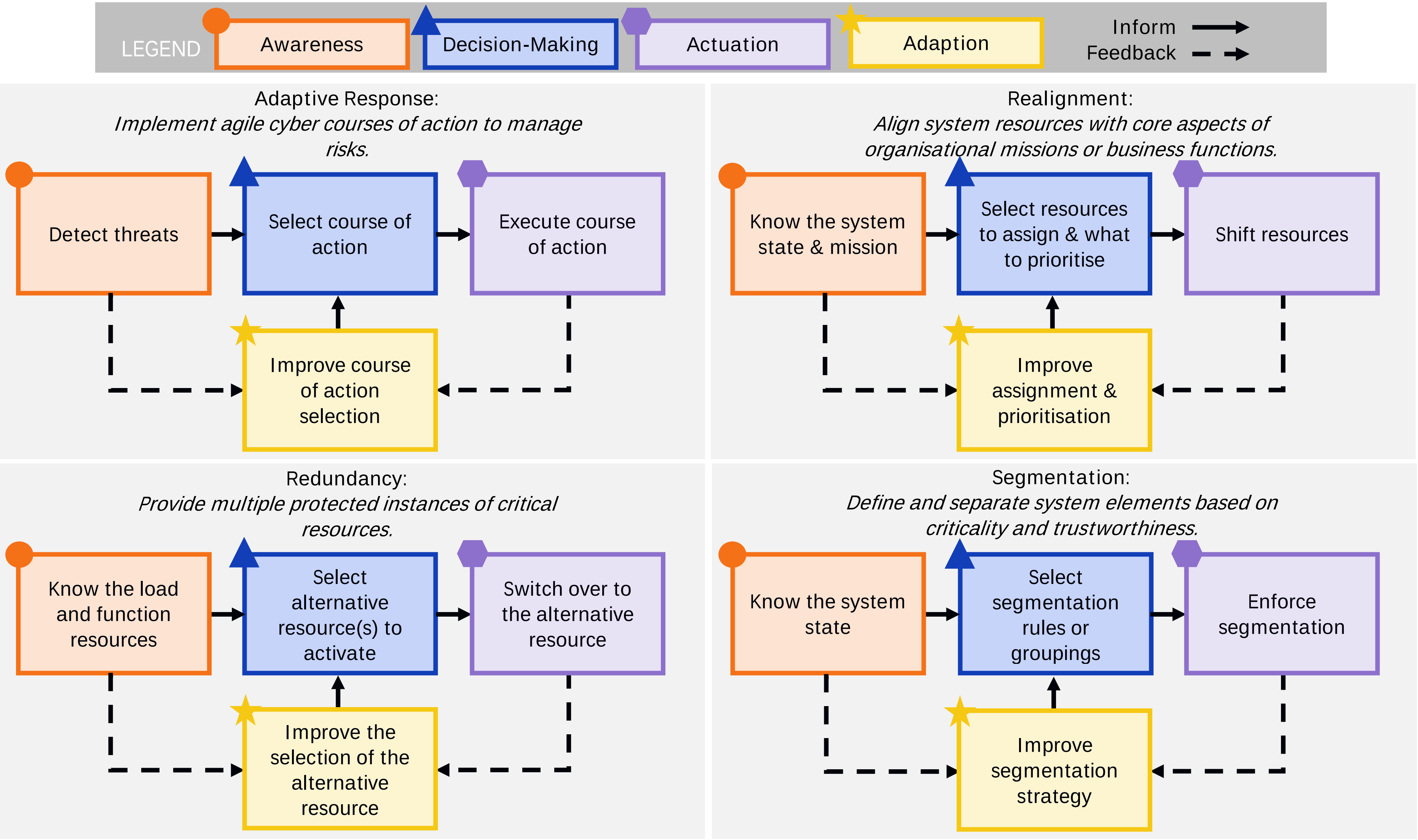

LEGEND
Awareness
Decision-Making
Actuation
Adaption
Inform
Feedback
Adaptive Response:
Implement agile cyber courses of action to manage risks.
Detect threats
Select course of action
Execute course of action
Improve course of action selection
Realignment:
Align system resources with core aspects of organisational missions or business functions.
Know the system state & mission
Select resources to assign & what to prioritise
Shift resources
Improve assignment & prioritisation
Redundancy:
Provide multiple protected instances of critical resources.
Know the load and function resources
Select alternative resource(s) to activate
Switch over to the alternative resource
Improve the selection of the alternative resource
Segmentation:
Define and separate system elements based on criticality and trustworthiness.
Know the system state
Select segmentation rules or groupings
Enforce segmentation
Improve segmentation strategy

Figure 3.1: A conceptual model of the autonomous loop for each MITRE CREF technique, illustrating how to enable autonomy within the technique.

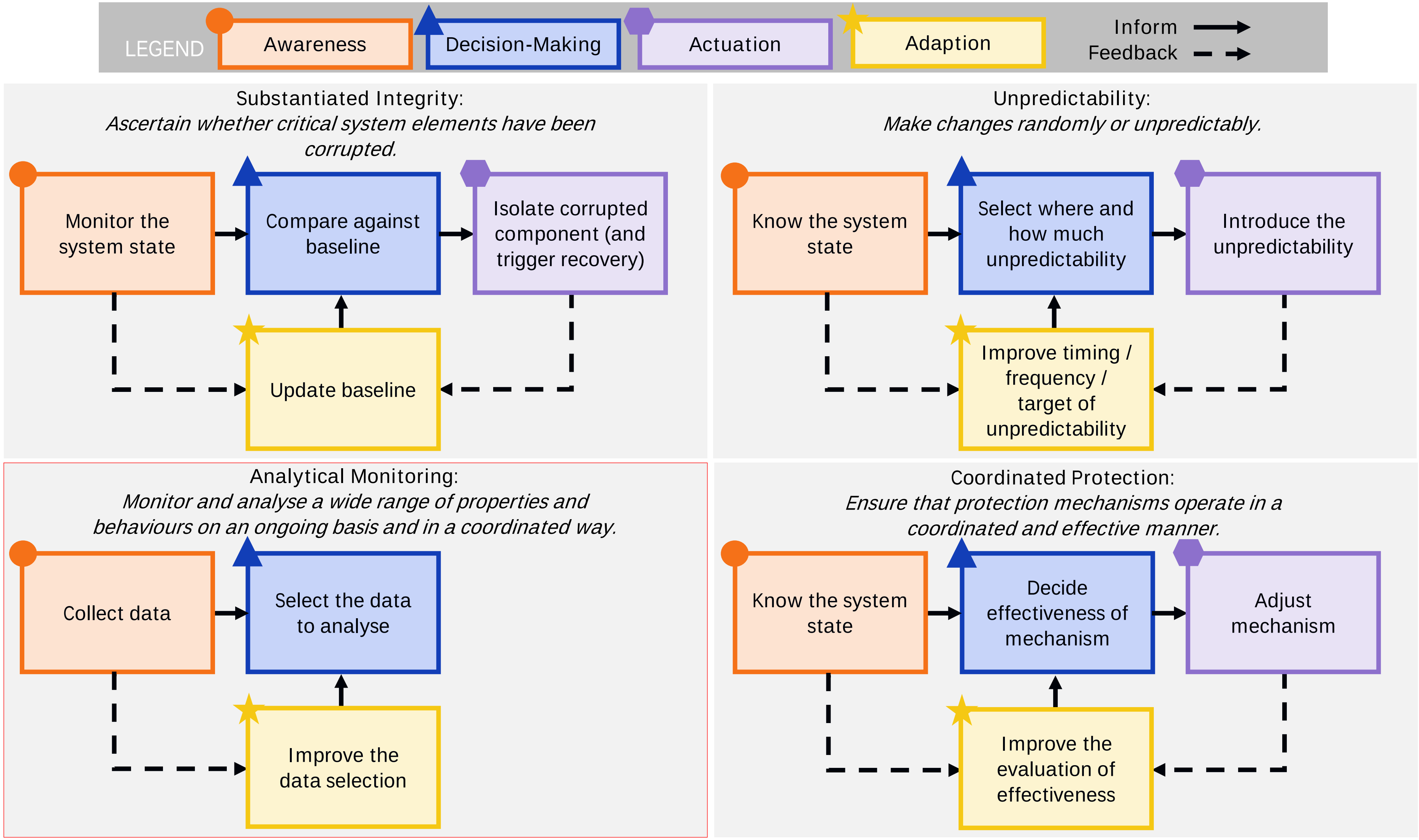

LEGEND
Awareness
Decision-Making
Actuation
Adaption
Inform
Feedback
Substantiated Integrity:
Ascertain whether critical system elements have been corrupted.
Monitor the system state
Compare against baseline
Isolate corrupted component (and trigger recovery)
Update baseline
Unpredictability:
Make changes randomly or unpredictably.
Know the system state
Select where and how much unpredictability
Introduce the unpredictability
Improve timing / frequency / target of unpredictability
Analytical Monitoring:
Monitor and analyse a wide range of properties and behaviours on an ongoing basis and in a coordinated way.
Collect data
Select the data to analyse
Improve the data selection
Coordinated Protection:
Ensure that protection mechanisms operate in a coordinated and effective manner.
Know the system state
Decide effectiveness of mechanism
Adjust mechanism
Improve the evaluation of effectiveness

Figure 3.2: A conceptual model of the autonomous loop for each MITRE CREF technique, illustrating how to enable autonomy within the technique (continued).

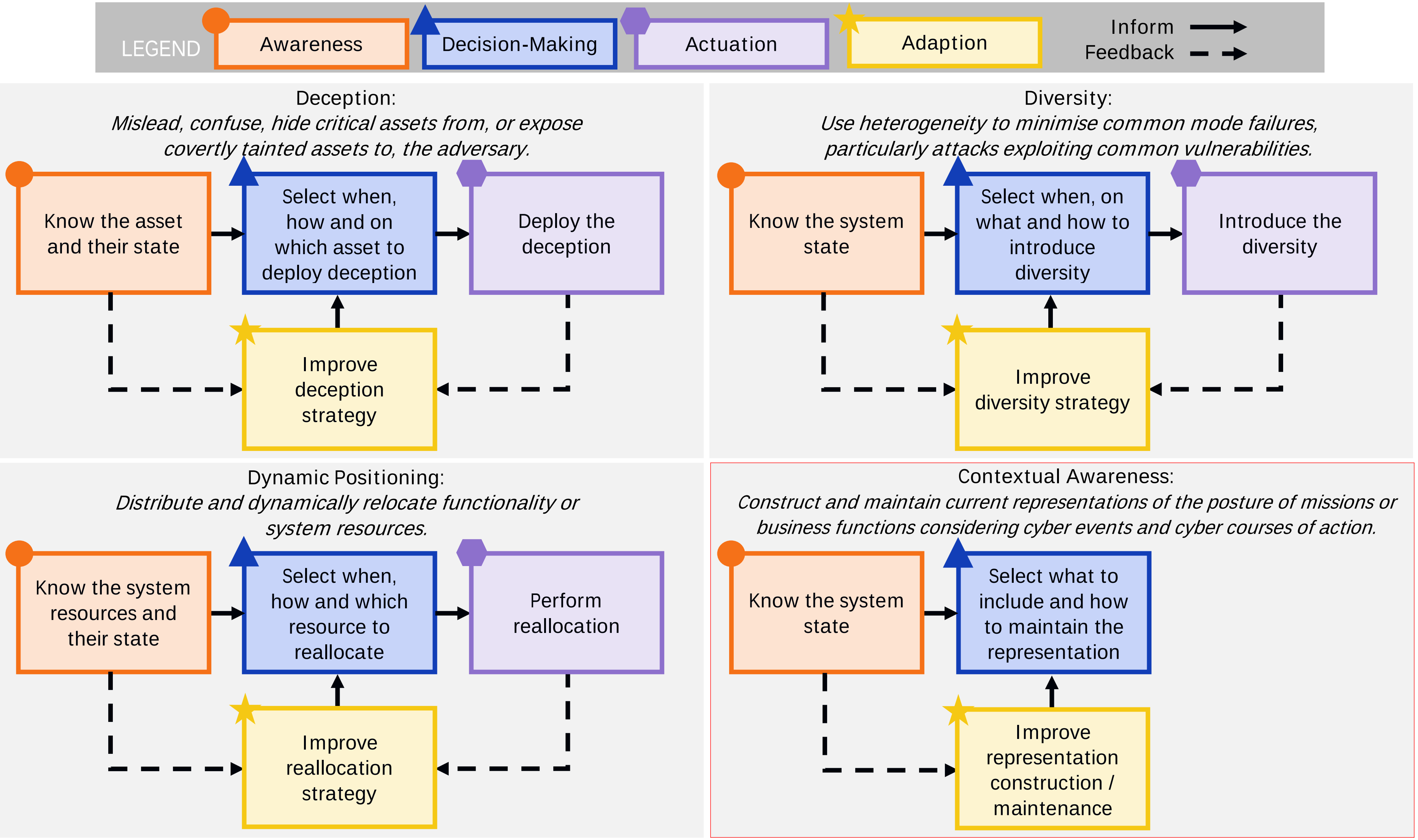

LEGEND
Awareness
Decision-Making
Actuation
Adaption
Inform
Feedback
Deception:
Mislead, confuse, hide critical assets from, or expose covertly tainted assets to, the adversary.
Know the asset and their state
Select when, how and on which asset to deploy deception
Deploy the deception
Improve deception strategy
Diversity:
Use heterogeneity to minimise common mode failures, particularly attacks exploiting common vulnerabilities.
Know the system state
Select when, on what and how to introduce diversity
Introduce the diversity
Improve diversity strategy
Dynamic Positioning:
Distribute and dynamically relocate functionality or system resources.
Know the system resources and their state
Select when, how and which resource to reallocate
Perform reallocation
Improve reallocation strategy
Contextual Awareness:
Construct and maintain current representations of the posture of missions or business functions considering cyber events and cyber courses of action.
Know the system state
Select what to include and how to maintain the representation
Improve representation construction / maintenance

Figure 3.3: A conceptual model of the autonomous loop for each MITRE CREF technique, illustrating how to enable autonomy within the technique (continued).

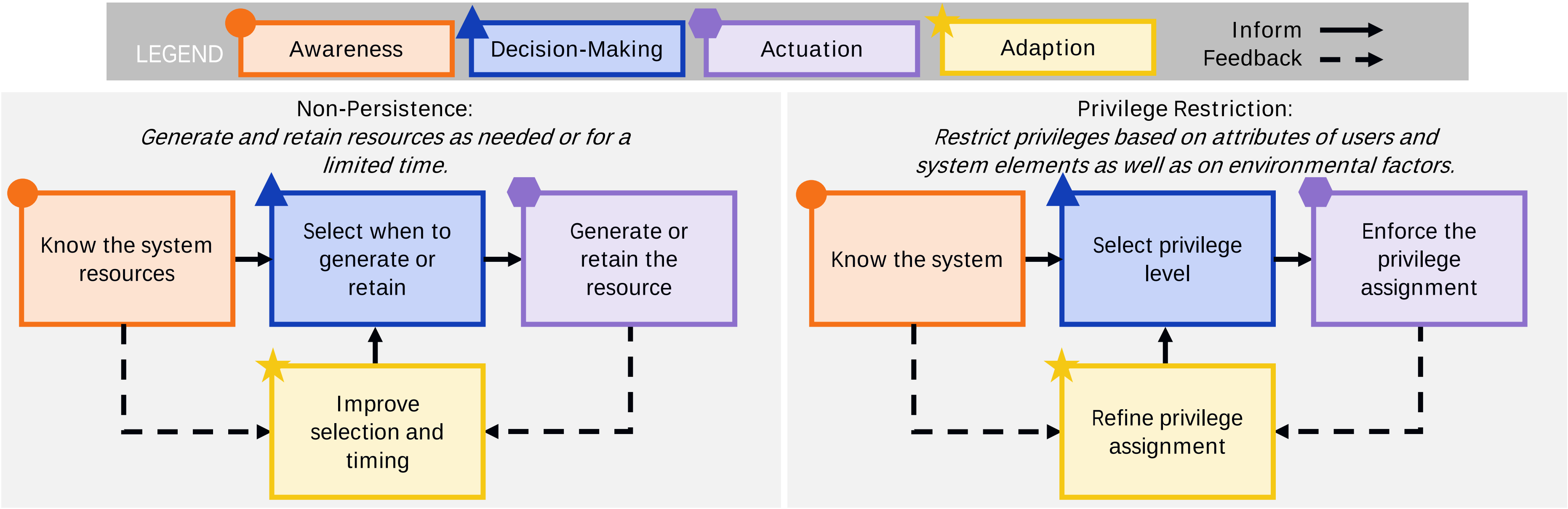

LEGEND
Awareness
Decision-Making
Actuation
Adaption
Inform
Feedback
Non-Persistence:
Generate and retain resources as needed or for a limited time.
Know the system resources
Select when to generate or retain
Generate or retain the resource
Improve selection and timing
Privilege Restriction:
Restrict privileges based on attributes of users and system elements as well as on environmental factors.
Know the system
Select privilege level
Enforce the privilege assignment
Refine privilege assignment

Figure 3.4: A conceptual model of the autonomous loop for each MITRE CREF technique, illustrating how to enable autonomy within the technique (continued).

These models serve as a foundation for assessing the autonomy potential of each CREF technique and identifying implementation gaps. Important to emphasise is that these models are not prescriptive or exhaustive. They represent a possible pathway to autonomy, abstracted to remain broadly applicable across different domains. Other architectures or mechanisms may also support autonomy, depending on system constraints, operational environments, or technological maturity.

Moreover, the *autonomy techniques* may exhibit overlap in their components. In practice, multiple techniques can be informed by a shared capability — such as a system-wide component that maintains and disseminates state awareness across all autonomous functions. This shared informational backbone enables coordinated decision-making and adaptation, reinforcing the system's overall resilience.

Such design philosophy is reflected in the techniques of *Contextual Awareness* and *Analytical Monitoring*, which inherently lack actuation capabilities. As a result, based on the definition of autonomy, they cannot be fully autonomised in isolation. However, their role is foundational: they provide the critical input and situational understanding required for the other techniques to function autonomously. In this sense, they act as enablers of autonomy rather than autonomy techniques themselves.

Furthermore, the *autonomy techniques* offer a structured lens for positioning CREF approaches within the techniques. Yet, it is important to recognise that many approaches do not align exclusively with a single (autonomous) capability. Instead, they often span multiple capabilities on their implementation and context. This multidimensional nature complicates straightforward classification and suggests that further research is needed to refine the criteria for positioning approaches within the loop.

In fact, this complexity may indicate that the MITRE CREF is not necessarily the most optimal foundation for developing A-CREF. A more suitable framework might require a reconfiguration or integration of multiple resilience engineering models to better accommodate the dynamic and overlapping nature of autonomous functions. Such refinements would support a more precise and adaptable operationalisation of autonomy in cyber resilience engineering.

4 Improvements & Future Directions

This chapter presents a set of suggestions to enhance the initial steps taken towards the Autonomous Cyber Resilience Engineering Framework (A-CREF), as briefly introduced in Section 4.1. These suggestions aim to refine the framework's conceptual foundations, expand its applicability, and address observed limitations. In Section 4.2, potential future directions are outlined to guide continued development of A-CREF. Together, the improvements and future steps form a roadmap for evolving A-CREF into a robust and adaptable framework for autonomous cyber resilience.

4.1 Enhancing Current Work

Granularity of Autonomous Capabilities

While the current framework adopts a high-level categorisation of autonomous capabilities, alternative models such as the Root Autonomous Capabilities (RACs) proposed by NIST offer more granular breakdowns [21]. For instance, Awareness may be decomposed into perceiving, sensing, and communicating. Exploring these finer-grained categories could improve the precision of autonomy assessments and better capture the nuances of implementation. Future iterations of A-CREF should experiment with such decompositions to determine whether they offer more suitable mappings for identifying autonomy potential.

Integration Alternative Resilience Framework

Although the MITRE CREF serves as the foundation for this work, other resilience engineering frameworks exist and may offer complementary perspectives. As briefly discussed in Section 1.2, these frameworks vary in scope, structure, and emphasis. A more in-depth comparative analysis is needed to evaluate whether a hybrid approach — combining elements from multiple frameworks — or an alternative foundation may be more appropriate for guiding autonomous cyber resilience engineering. This could lead to a more flexible and domain-adaptable A-CREF.

4.2 Future Research Directions

Integration ACR Design Principles

In [22], six design principles for ACR are introduced, including nested defence, which distinguishes between fast-reactive (System I) and slow-deliberative (System II) layers. Future work should explore how these principles can be embedded within A-CREF — either as foundational design elements or as complementary guidance alongside the ACR. This could enhance the framework's applicability to real-world system architectures.

Technological Enablers and Flexibility

While this work identifies the autonomy potential of CREF techniques, realising autonomous resilience in practice requires identifying the technological enablers for each capability. These may include AI agents, orchestration platforms, or adaptive control systems. Moreover, the framework must remain flexible to accommodate emerging technologies. For instance, the rise of agentic AI — though not yet mature — could significantly expand the scope and feasibility of autonomous functionality.

Autonomy Across Resilience Order

Literature suggests that resilience strategies can be organised into first-order (robustness), second-order (short-term), and third-order (long-term) resilience [23]. Investigating how autonomy manifests differently across these orders could provide deeper insight into the design and evaluation of autonomous systems. For example, autonomy in third-order resilience may require more strategic planning and learning capabilities than in first-order robustness.

Balancing Operational Goals and Costs

As highlighted in [24], enabling resilience involves trade-offs between operational goals and costs. A similar quantitative analysis should be conducted for autonomous resilience, examining how autonomy affects system performance, resource consumption, and risk exposure. This would support informed decision-making in system design and deployment.

Domain-Specific Criteria Variation

Autonomous resilience requirements may vary significantly across domains such as telecommunications, healthcare, and finance. Research is needed to determine how generic the *Autonomy Criteria* can remain while still being effective across sectors. For example, real-time autonomy may be feasible in telecom but constrained in healthcare due to regulatory oversight. Including domain-specific examples could help illustrate these differences and guide tailored framework adaptations.

5 References

[1] W. S. Admass, Y. Y. Munaye and A. A. Diro, “Cyber security: State of the art, challenges and future directions,” *Cyber Security and Applications,* vol. 2, p. 100031, 2024.

[2] B. Gijsen, R. Montalto, J. Panneman, F. Falconieri, P. Wiper and P. Zuraniewski, “Self-healing for cyber-security,” *IEEE 2021 Sixth International Conference on Fog and Mobile Edge Computing (FMEC),* pp. 1-7, 2021.

[3] A. Kovačević, N. Putnik and O. Tošković, “Factors related to cyber security behavior,” *IEEE Access,* vol. 8, pp. 125140-125148, 2020.

[4] TNO Project Team Self-Healing Systems By Design, “Roadmap for Autonomous Resilience,” 2024.

[5] P. Arcaini, E. Riccobene and P. Scandurra, “Modeling and analyzing MAPE-K feedback loops for self-adaptation,” *2015 IEEE/ACM 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems,* pp. 13-23, 2015.

[6] NIST, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” *Special Publication 800-160,* vol. 2, 2019.

[7] J. Rak and D. Hutchison, Guide to disaster-resilient communication networks, Eds: Springer Nature, 2020.

[8] P. Smith, D. Hutchison, J. P. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. La and B. Plattner, “Network resilience: a systematic approach,” *IEEE Communications Magazine,* vol. 49, no. 7, pp. 88-97, 2011.

[9] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller and P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” *Computer networks,* vol. 54, no. 8, pp. 1245-1265, 2010.

[10] International Telecommunication Union (ITU), “IMT-2030 Framework: Recommendation ITU-R M.2160-0,” ITU-R Working Party 5D, Nov 2023.

[11] L. Khaloopour, Y. Su, F. Raskob, T. Meuser, R. Bless, L. Janzen, ... and V. Jamali, “Resilience-by-design in 6G networks: Literature review and novel enabling concepts,” *IEEE access,* vol. 12, pp. 155666-155695, 2024.

[12] R. J. Reifert, Y. Karacora, C. Chaccour, A. Sezgin and W. Saad, “Resilience and criticality: Brothers in arms for 6G,” *arXiv preprint arXiv:2412.03661,* pp. 1-23, 2024.

[13] N. H. Mahmood, S. Samarakoon, P. Porambage, M. Bennis and M. Latva-aho, “Resilient-by-design: A resiliency framework for future wireless networks,” *arXiv preprint arXiv:2410.23203,* pp. 1-7, 2024.

[14] K. Shortridge, Security chaos engineering: sustaining resilience in software and systems, O'Reilly Media, Inc., 2023.

[15] MITRE, “CREF Navigator,” [Online]. Available: https://crefnavigator.mitre.org/navigator. [Accessed 2025].

[16] M. Müller, T. Müller, A. Talkhestani, M. P. B., N. Jazdi and M. Weyrich, *at-Automatisierungstechnik,* vol. 69, no. 1, pp. 3-13, 2021.

[17] NATO, “Autonomous systems: Issues for defence policymakers,” *Innovation in Capability Development,* vol. 2, 2015.

[18] S. A. Mostafa, M. S. Ahmad and A. Mustapha, “Adjustable autonomy: a systematic literature review,” *Artificial Intelligence Review,* vol. 51, no. 2, pp. 149-186, 2019.

[19] NIST, “Artificial Intelligence Risk Management Framework (AI RMF 1.0),” pp. 100-1, 2023.

[20] Q. Song, E. Engström and P. Runeson, “Concepts in Testing of Autonomous Systems: Academic literature and industry practice,” *2021 IEEE/ACM 1st Workshop on AI Engineering-Software Engineering for AI (WAIN),* pp. 74-81, 2021.

[21] NIST, “Autonomy Levels For Unmanned Systems (ALFUS) Framework,” *NIST Special Publication 1011-II-1.0 Framework Models,* vol. 2, no. 1, pp. 1-73, 2007.

[22] S. Finner, S. Kumarswamy-Das and B. Gijsen, “Self-Healing by design: Immune-system inspired autonomous cyber resilience,” in *MAST Australia 2024*, Adelaide, 2024.

[23] R. J. Reifert, Y. Karacora, C. Chaccour, A. Sezgin and W. Saad, “Resilience and criticality: Brothers in arms for 6G,” *arXiv preprint arXiv:2412.03661,* pp. 1-23, 2024.

[24] X. Cadet, S. Boboila, E. Koh, P. Chin and A. Oprea, “Quantitative Resilience Modeling for Autonomous Cyber Defense,” *arXiv preprint arXiv:2503.02780,* pp. 1-17, 2025.

[25] N. Tomatis, “BlueBotics: navigation for the clever robot,” *IEEE robotics & automation magazine,* vol. 18, no. 2, pp. 14-16, 2011.

[26] B. Rinner, C. Bettstetter, H. Hellwagner and S. Weiss, “Multidrone systems: More than the sum of the parts,” *Computer,* vol. 54, no. 5, pp. 34-43, 2021.

[27] E. Aguado, Z. Milosevic, C. Hernández, R. Sanz, M. Garzon, D. Bozhinoski and C. Rossi, “Functional self-awareness and metacontrol for underwater robot autonomy,” *Sensors,* vol. 21, no. 4, p. 1210, 2021.

[28] M. Petrlík, T. Báča, D. Heřt, M. Vrba, T. Krajník and M. Saska, “A robust UAV system for operations in a constrained environment,” *IEEE Robotics and Automation Letters,* vol. 5, no. 2, pp. 2169-2176, 2020.

[29] D. McColl, C. Jiang and G. Nejat, “Classifying a person’s degree of accessibility from natural body language during social human–robot interactions,” *IEEE transactions on cybernetics,* vol. 47, no. 2, pp. 524-538, 2016.

[30] S. Yang, Y. Huang, L. Li, S. Feng, X. Na, H. Chen and A. Khajepour, “How to guarantee driving safety for autonomous vehicles in a real-world environment: A perspective on self-evolution mechanisms,” *IEEE Intelligent Transportation Systems Magazine,* vol. 16, no. 2, pp. 41-54, 2024.

[31] R. K. Vithanage, C. S. Harrison and A. K. De Silva, “Autonomous rolling-stock coupler inspection using industrial robots,” *Robotics and Computer-integrated Manufacturing,* vol. 59, pp. 82-91, 2019.

[32] W. Jitviriya, P. Chaicherdkiat, N. Pudchuen and E. Hayashi, “Development of Automation Recognition of Hazmat Marking Chart for Rescue Robot,” *Journal of Robotics, Networking and Artificial Life,* vol. 5, no. 4, pp. 223-227, 2019.

[33] M. Chowdhury, A. Khandakar, S. Ahmed, F. Al-Khuzaei, J. Hamdalla, F. Haque, M. Reaz, A. Al Shafei and N. Al-Emadi, “Design, construction and testing of IoT based automated indoor vertical hydroponics farming test-bed in Qatar,” *Sensors,* vol. 20, no. 19, p. 5637, 2020.

[34] T. Kominami, H. Paul and K. Shimonomura, “Detection and localization of thin vertical board for UAV perching,” *Journal of Robotics and Mechatronics,* vol. 35, no. 2, pp. 398-407, 2023.

[35] T. M. Dawdi, N. Abdalla, Y. M. Elkalyoubi and B. Soudan, "Locating victims in hot environments using combined thermal and optical imaging," *Computers & Electrical Engineering,* vol. 85, p. 106697, 2020.

[36] J. Kim, "Automatic Control of a Sunlight Reflector Board for Achieving the Sunlight Intensity Set by the Greenhouse Operator," *Applied Sciences,* vol. 14, no. 12, p. 5257, 2024.

[37] M. Kang, S. Joe, T. An, H. Jang and B. Kim, "A novel robotic colonoscopy system integrating feeding and steering mechanisms with self-propelled paddling locomotion: A pilot study," *Mechatronics,* vol. 73, p. 102478, 2021.

[38] S. Vasanthapriyan and V. Randima, "Design IoT based smart electricity power saving university: Analysis from a lecture hall," *Journal of Computer Science,* vol. 15, no. 8, pp. 1097-1107, 2019.

[39] A. Khan, S. Rehman, M. Waleed, A. Khan, U. Khan, T. Kamal, S. K. Afridi and S. N. K. Marwat, "Forensic video analysis: passive tracking system for automated Person of Interest (POI) localization," *IEEE,* vol. 6, pp. 43392-43403, 2018.

[40] S. A. Shaban, "A smart system for the university chemical laboratory using iot," *Journal of Advances in Information Technology,* vol. 15, no. 1, pp. 104-117, 2024.

[41] K. Nakamura, T. Funatomi, A. Hashimoto, M. Ueda and M. Minoh, "Development and evaluation of near real-time automated system for measuring consumption of seasonings," *IEICE TRANSACTIONS on Information and Systems,* vol. 98, no. 12, pp. 2229-2241, 2015.

[42] A. Kumar and H. Rajagopal, "Automated seeding and irrigation system using Arduino," *Journal of Robotics, Networking and Artificial Life,* vol. 8, no. 4, pp. 259-262, 2022.

[43] M. Díaz-Choque, C. Dávila-Ignacio, A. Sanchez-Ayte, G. Morales-Romero, A. Torres-Quiroz, N. Alvarado-Bravo and F. Aldana-Trejo, "Automated system for monitoring and control of the liquid wax production process," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 23, no. 2, pp. 782-790, 2021.

[44] T. E. Liang, U. U. Sheikh and M. N. H. Mohd, "Malaysian car plate localization using region-based convolutional neural network," *Bulletin of Electrical Engineering and Informatics,* vol. 9, no. 1, pp. 411-419, 2020.

[45] Y. Gao, Z. Chen, J. Lin, X. Li and Y. H. Liu, "Development of an automated system for the soldering of USB cables," *Robotics and Computer-Integrated Manufacturing,* vol. 79, p. 102440, 2023.

[46] L. A. Cruz Salazar and B. Vogel-Heuser, "A CPPS-architecture and workflow for bringing agent-based technologies as a form of artificial intelligence into practice," *at-Automatisierungstechnik,* vol. 70, no. 6, pp. 580-598, 2022.

[47] M. Houbraken, S. Logghe, M. Schreuder, P. Audenaert, D. Colle and M. Pickavet, "Automated Incident Detection Using Real-Time Floating Car Data," *Journal of Advanced Transportation,* vol. 2017, no. 1, p. 8241545, 2017.

[48] X. Wu, K. Liu, J. Zhang, Z. Yuan, J. Liu and Q. Yu, "An Optimized Collision Avoidance Decision-Making System for Autonomous Ships under Human-Machine Cooperation Situations," *Journal of Advanced Transportation,* vol. 2021, no. 1, p. 7537825, 2021.

[49] Z. Gong, B. K. Chen, J. Liu and Y. Sun, "Robotic probing of nanostructures inside scanning electron microscopy," *IEEE Transactions on Robotics,* vol. 30, no. 3, pp. 758-765, 2014.

[50] N. Lüling, J. Straub, A. Stana, M. Brodbeck, D. Reiser, P. Berner and H. W. Griepentrog, "Development and evaluation of a self-adaptable planting unit for an autonomous

planting process of field vegetables," *Smart Agricultural Technology,* vol. 9, p. 100578, 2024.

[51] E. I. Epelle, M. Yaseen, A. Macfarlane, M. Cusack, A. Burns and L. Rolland, "Automation of large-scale gaseous ozonation: a case study of textile and PPE decontamination," *Sustainability,* vol. 15, no. 3, p. 2216, 2023.

[52] C. Otto, P. Zirker, T. Walther and F. Lenk, "A Flexible System for Stepwise Automation of Microbial Testing of Drinking and Process Water," *SLAS TECHNOLOGY: Translating Life Sciences Innovation,* vol. 26, no. 5, pp. 532-544, 2021.

[53] A. C. García, C. A. P. Alban, J. R. T. Benalcázar, A. C. Rodríguez, L. L. Lorente-Leyva and A. M. L. Aleaga, "Control of pollutant emissions from a boiler through the percentage of oxygen," *Journal Européen des Systèmes Automatisés,* vol. 54, no. 3, pp. 469-474, 2021.

[54] Y. Cheng, Y. Huang, B. Pang and W. Zhang, "ThermalNet: A deep reinforcement learning-based combustion optimization system for coal-fired boiler," *Engineering Applications of Artificial Intelligence,* vol. 74, pp. 303-311, 2018.

[55] T. Arai, Y. Aiyama, M. Sugi and J. Ota, "Holonic assembly system with Plug and Produce," *Computers in Industry,* vol. 46, no. 3, pp. 289-299, 2001.

[56] Y. Zhai, Z. Hu, Q. Wang, Q. Yang and K. Yang, "Multi-geometric reasoning network for insulator defect detection of electric transmission lines," *Sensors,* vol. 22, no. 16, p. 6102, 2022.

[57] R. Atiqur, "iPark: automated smart parking system," *Int J Adv Appl Sci,* vol. 10, no. 2, pp. 107-114, 2021.

[58] S. Matsuda, M. Saito, H. Masuda, K. Yoon, M. Wada and H. Hashimoto, "On human factor issues in the parking assistance system design," *ITSC2000. 2000 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.00TH8493),* pp. 434-439, 2002.

[59] L. Cao, "Beyond AutoML: mindful and actionable AI and AutoAI with mind and action," *IEEE Intelligent Systems,* vol. 37, no. 5, pp. 6-18, 2022.

[60] J. Svensson, "Artificial intelligence is an oxymoron: The importance of an organic body when facing unknown situations as they unfold in the present moment," *AI & society,* vol. 38, no. 1, pp. 363-372, 2023.

[61] M. F. Hansen, M. L. Smith, L. N. Smith, K. A. Jabbar and D. Forbes, "Automated monitoring of dairy cow body condition, mobility and weight using a single 3D video capture device," *Computers in industry,* vol. 98, pp. 14-22, 2018.

[62] Á. Takács, I. Rudas, D. Bösl and T. Haidegger, "Highly automated vehicles and self-driving cars [industry tutorial]," *IEEE Robotics & Automation Magazine,* vol. 25, no. 4, pp. 106-112, 2018.

[63] B. R. Sundaram, E. Aravind, S. Harithaa, G. Karthick and S. K. Vasudevan, "Revolutionizing Technology Prioritizing Emergency Vehicles In Traffic," *Research Journal of Applied Sciences, Engineering and Technology,* vol. 8, no. 7, pp. 886-891, 2014.

[64] T. K. M. Nagatsuma, K. Yamamoto, T. Tsugawa, H. Kitauchi, T. Kondo, H. Ishibashi, M. Nishioka and M. Okada, "Operation of a Data Acquisition, Transfer, and Storage System for the Global Space-Weather Observation Network," *Data Science Journal,* vol. 13, pp. 51-56, 2014.

[65] G. Aguiar Noury, A. Walmsley, R. B. Jones and S. E. Gaudl, "The barriers of the assistive robotics market—What inhibits health innovation?," *Sensors,* vol. 21, no. 9, p. 3111, 2021.

[66] D. Pantförder, B. Vogel-Heuser, D. Gramß and K. Schweizer, “Supporting operators in process control tasks—benefits of interactive 3-D visualization,” *IEEE Transactions on Human-Machine Systems,* vol. 46, no. 6, pp. 895-907, 2016.

[67] M. Zoubir, B. Schwarz, J. Heidinger, M. Gruner, H. C. Jetter and T. Franke, “Anchoring autonomy: understanding seafarers’ interaction with energy efficiency decision support systems for route planning and the role of basic psychological needs,” *Cognition, Technology & Work,* pp. 1-16, 2025.

[68] T. Nikonova, Ł. Gierz, O. Zharkevich, E. Dandybaev, M. Baimuldin, L. Daich and A. E. Sichkarenko, “Control of Physical Processes in an Extrusion Line Polymer Sleeves Production,” *Applied Sciences,* vol. 12, no. 20, p. 10309, 2022.

[69] C. Barrett-Pink, L. Alison, S. Maskell and N. Shortland, “On the bridges: Insight into the current and future use of automated systems as seen by Royal Navy personnel,” *Journal of cognitive engineering and decision making,* vol. 13, no. 3, pp. 127-145, 2019.

[70] N. Panda and B. K. Pattanayak, “Defense against co-operative black-hole attack and gray-hole attack in MANET,” *International Journal of Engineering & Technology,* vol. 7, no. 3.4, pp. 84-89, 2018.

[71] N. N. Zheng, Z. Y. Liu, P. J. Ren, Y. Q. Ma, S. T. Chen, S. Y. Yu, J. Xue, B. Chen and F. Y. Wang, “Hybrid-augmented intelligence: collaboration and cognition,” *Frontiers of Information Technology & Electronic Engineering,* vol. 18, no. 2, pp. 153-179, 2017.

[72] T. Stirling, S. Wischmann and D. Floreano, “Energy-efficient indoor search by swarms of simulated flying robots without global information,” *Swarm Intelligence,* vol. 4, no. 2, pp. 117-143, 2010.

[73] L. Xi, Z. Peng, L. Jiao and B. M. Chen, “Smooth quadrotor trajectory generation for tracking a moving target in cluttered environments,” *Science China Information Sciences,* vol. 64, no. 7, p. 172209, 2021.

[74] X. You, C. X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang, M. Zhu, B. Sheng, D. Wang, Z. Pan, P. Zhu, Y. Yang, Z. Liu, P. Zhang, X. Tao, S. Li, Z. Chen, X. Ma, C. I, S. Han and Y. C. Liang, “Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts,” *Science China information sciences,* vol. 64, no. 1, p. 110301, 2021.

[75] Y. Wang, Z. Sun, H. Zhang, W. Cui, K. Xu, X. Ma and D. Zhang, “Datashot: Automatic generation of fact sheets from tabular data,” *IEEE transactions on visualization and computer graphics,* vol. 26, no. 1, pp. 895-905, 2019.

[76] J. D. Filoteo-Razo, O. X. Vera-Duarte, J. M. Estudillo-Ayala, J. C. Hernandez-Garcia, D. Jauregui-Vazquez, J. R. Martinez-Angulo, J. Elizondo-Leal and R. Rojas-Laguna, “U-shaped plastic fiber optic sensor for measuring adulteration in liquids via RGB color changes,” *IEEE Sensors Letters,* vol. 5, no. 12, pp. 1-4, 2021.

[77] X. Du, X. Pan, Y. Cao, B. He, G. Fan, Y. Chen and D. Xu, “Flowcog: Context-aware semantic extraction and analysis of information flow leaks in android apps,” *IEEE Transactions on Mobile Computing,* vol. 22, no. 11, pp. 6460-6476, 2022.

[78] W. H. Wang, X. Y. Liu and Y. Sun, “High-throughput automated injection of individual biological cells,” *IEEE Transactions on automation science and engineering,* vol. 6, no. 2, pp. 209-219, 2008.

[79] A. Bs, A. V. Gk, S. Rao, M. Beniwal and H. J. Pandya, “Electrical phenotyping of human brain tissues: An automated system for tumor delineation,” *IEEE Access,* vol. 10, pp. 17908-17919, 2022.

[80] S. Ullas, B. U. Maheswari, S. Ponnekanti and T. M. Kumar, “Automated System to Optimise the Process and Energy Consumption for Sewage Treatment Plant based on

Gas Emission by using Sensors and IoT," *IEEE Access,* vol. 13, pp. 115972-115989, 2025.

[81] E. T. R. Babar and M. U. Rahman, "A smart, low cost, wearable technology for remote patient monitoring," *IEEE Sensors Journal,* vol. 21, no. 19, pp. 21947-21955, 2021.

[82] Z. Shen, A. Nacev, A. Sarwar, R. Lee, D. Depireux and B. Shapiro, "Automated fluorescence and reflectance coregistered 3-D tissue imaging system," *IEEE transactions on magnetics,* vol. 49, no. 1, pp. 279-284, 2012.

[83] G. Zamzmi, R. Kasturi, D. Goldgof, R. Zhi, T. Ashmeade and Y. Sun, "A review of automated pain assessment in infants: features, classification tasks, and databases," *IEEE reviews in biomedical engineering,* vol. 11, pp. 77-96, 2017.

Appendix A
Search Query

This appendix presents the search queries provided to the respective databases. Section A.1 displays the query used for Scopus and SpringerLink. Section A.2 outlines the query applied to the IEEE database.

A.1 Scopus & SpringerLink

PUBYEAR > 1999 AND ABS(“autonomous system” OR “automated system” OR “unmanned system”) AND NOT TITLE-ABS-KEY (algorithm OR method OR methodology OR approach OR model OR technique OR "theor*" OR conceptual OR strategy OR framework OR review OR survey OR application OR service OR software OR tool OR program OR dataset OR database OR function OR chatbot OR simulation) AND (EXCLUDE (AFFILCOUNTRY,"United States")) AND (EXCLUDE (PREFNAMEAUID,"undefined")) AND (LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (LANGUAGE,"English"))

A.2 IEEE

("Abstract":"autonomous system " OR "Abstract":"automated system" OR "Abstract":"unmanned system")

AND NOT

(("Abstract":"algorithm" OR "Abstract":"method" OR "Abstract":"methodology" OR "Abstract":"approach" OR "Abstract":"model" OR "Abstract":"technique" OR "Abstract":"theor*" OR "Abstract":"conceptual" OR "Abstract":"strategy" OR "Abstract":"framework" OR "Abstract":"review" OR "Abstract":"survey" OR "Abstract":"application" OR "Abstract":"service" OR "Abstract":"software" OR "Abstract":"tool" OR "Abstract":"program" OR "Abstract":"dataset" OR "Abstract":"database" OR "Abstract":"function" OR "Abstract":"chatbot" OR "Abstract":"simulation")

OR

("Index Terms":"algorithm" OR "Index Terms":"method" OR "Index Terms":"methodology" OR "Index Terms":"approach" OR "Index Terms":"model" OR "Index Terms":"technique" OR "Index Terms":"theor*" OR "Index Terms":"conceptual" OR "Index Terms":"strategy" OR "Index Terms":"framework" OR "Index Terms":"review" OR "Index Terms":"survey" OR "Index Terms":"application" OR "Index Terms":"service" OR "Index Terms":"software" OR "Index Terms":"tool" OR "Index Terms":"program" OR "Index Terms":"dataset" OR "Index Terms":"database" OR "Index Terms":"function" OR "Index Terms":"chatbot" OR "Index Terms":"simulation")

OR

("Document Title":"algorithm" OR "Document Title":"method" OR "Document Title":"methodology" OR "Document Title":"approach" OR "Document Title":"model" OR "Document Title": "technique" OR "Document Title":"theor*" OR "Document Title":"conceptual" OR "Document Title":"strategy" OR "Document Title":"framework" OR "Document Title":"review" OR "Document Title":"survey" OR "Document Title":"application" OR "Document Title":"service" OR "Document Title":"software" OR "Document Title":"tool" OR "Document Title":"program" OR "Document Title":"dataset" OR "Document Title":"database" OR "Document Title":"function" OR "Document Title":"chatbot" OR "Document Title":"simulation")

OR

("Publication Title":"algorithm" OR "Publication Title":"method" OR "Publication Title":"methodology" OR "Publication Title":"approach" OR "Publication Title":"model" OR "Publication Title":"technique" OR "Publication Title":"theor*" OR "Publication Title":"conceptual" OR "Publication Title":"strategy" OR "Publication Title":"framework" OR "Publication Title":"review" OR "Publication Title":"survey" OR "Publication Title":"application" OR "Publication Title":"service" OR "Publication Title":"software" OR "Publication Title":"tool" OR "Publication Title":"program" OR "Publication Title":"dataset" OR "Publication Title":"database" OR "Publication Title":"function" OR "Publication Title":"chatbot" OR "Publication Title":"simulation"))

Appendix B
Review Prompt

In this appendix, the review prompt is provided that has been used as prompt fed into CoPilot to extract details on a specific paper.

```
First of all, you do not need to have answers, be restrictive. When
answering question, use only the information from the research paper
provided. Be critical, it is not obliged that the answer is present.
If you cannot find an answer based on the given paper, please respond
with “The research paper does not contain a clear answer to this
question.”

1 GENERAL INFORMATION
(1.1) Author(s)
(1.2) Name of journal
(1.3) Publication year
(1.4) Domain
(1.5) Relevance of the study, please answer with YES or NO (Relevance
of the paper for answering the research question based on the
following categories):
A: Considers a deployed system
B: Introduces an autonomous aspect
C: Mentions what the introduction of the autonomous aspect adds for
capabilities to the system

2 DEPTH:
(2.0) Phrase the system (including purpose) in 3-5 words
(2.1) Which/What components were added to the system to achieve
autonomy
(2.2) What autonomous functionality was achieved by introducing the
component identified in (2.1).
(2.3) Classify the functionality under (Awareness ; Decision-Making ;
Adaption ; Actuation). Preferably, assign each functionality to a
single concept but if it more suitable to assign it to more, please
do so and give a short argument why. Please be aware that you are not
forced to be able to classify functionalities under a concept. If you
are not able to please respond with “Unable2Map”.

Order DEPTH (2.1), (2.2) and (2.3) in a single tabular format.

The research paper:
```

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life