A reference architecture for digital immune systems

Kay Smarsly[1,2][0000−0001−7228−3503]

[1] Hamburg University of Technology, Institute of Digital and Autonomous Construction, Blohmstraße 15, 21079 Hamburg, Germany
[2] United Nations University (UNU) Hub on Engineering to Face Climate Change, United Nations University Institute for Water, Environment and Health (UNU-INWEH), Hamburg University of Technology, Germany
kay.smarsly@tuhh.de
http://www.tuhh.de/idac

Abstract. Modern structural health monitoring (SHM) systems and the physical structures being monitored constitute coupled cyber-physical systems that must be protected as a whole. As a consequence, threats no longer solely stem from structural anomalies, but also from internal SHM system faults and, in particular, from cyberattacks that may falsify sensor data, disrupt communication, or even sabotage critical infrastructure. The capabilities required to withstand the threats are often subsumed under the notion of a "digital immune system". However, prior work on digital immune systems either targets other application domains that cannot be directly transferred to civil infrastructure or uses the label "digital immune system" as a buzzword without systematically mapping biological immune functions to digital counterparts. This paper presents a biologically inspired reference architecture for digital immune systems for civil infrastructure, defines and formally specifies the threat categories relevant to coupled cyber-physical SHM systems, introduces a compact illustrative sensor-fault scenario, and derives implementation-oriented recommendations intended to support computational modeling and simulation. Explicitly drawing from the biological immune functions, the reference architecture includes innate and adaptive layers, distinguishing between cellular-oriented, local modules and humoral-oriented, global elements. The architecture is intended to serve as a generally applicable blueprint for designing digital immune systems for civil infrastructure, aiming to advance cyber-physical SHM systems at the interface between civil engineering and computer science.

Keywords: Digital immune systems · Artificial immune systems · Cyber-physical systems · Structural health monitoring · Fault diagnosis · Cyber-security · Computational modeling.

1 Introduction

Structural health monitoring (SHM) has emerged as a core methodology for ensuring safety, serviceability, and long-term sustainability of civil infrastructure

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

by enabling continuous, data-driven assessment of structural conditions [1]. For more than two decades, wireless sensor networks have been a key driver of SHM, enabling scalable, distributed-cooperative, and flexible on-site data acquisition and analysis [2], while machine-learning-based methods have expanded SHM from data collection to automated pattern recognition and decision-support [3]. Advances in sensing technologies, embedded computing, and data analytics have transformed SHM systems into complex systems composed of interconnected components [4]. Modern SHM systems are considered cyber-physical systems with dense sensor networks, embedded processing, communication links, and back-end services that form coupled systems comprising (i) the physical structures and (ii) the SHM systems [5]. In coupled cyber-physical SHM systems, threats no longer arise solely from structural anomalies (including damage) and SHM system faults (including sensor faults) [6], but also from cyberattacks that may aim to falsify sensor data, disrupt communication, or sabotage critical infrastructure. The combination of all capabilities required to withstand the new set of threat categories can be subsumed under the term "digital immune system", a concept that remains largely unfamiliar in civil engineering and, in particular, within SHM of civil infrastructure.

Digital immune systems in domains outside SHM have been proposed since the early 1990s, e.g. for automated detection, analysis, and containment of computer viruses in networked environments [7]. For example, in the financial domain, immune-inspired models have been developed for credit card fraud detection that mimic human immune responses to identify anomalous transactions [8]. Furthermore, immune-based frameworks have been applied to safeguard digital assets by simulating human immune mechanisms to assess and mitigate emerging risks in cryptocurrency platforms [9]. In the healthcare domain, artificial immune system algorithms have been devised for intrusion detection, aiming to protect Internet-of-Medical-Things devices by using immune-like anomaly recognition to secure patient data and device functionality [10]. In the industrial domain, biologically inspired algorithms have been integrated into industrial control systems (e.g., negative selection and dendritic cell techniques) to detect network anomalies and bolster resilience against cyberattacks in dynamic industrial networks [11]. In the cybersecurity domain, digital immune systems have been combined with artificial intelligence (AI), demonstrating improved threat detection accuracy and operational efficiency in security operations centers [12].

More recently, the term "digital immune system" has been adopted in industry analyst discourse to denote a managerial framework for improving software resilience, reliability, and operational stability rather than a biologically inspired system in a strict sense. For example, Gartner's digital immune system concept primarily aggregates established practices, such as DevSecOps (Development, Security, and Operations), as well as AI-assisted operations into a unifying narrative aiming at reducing software defects and business disruptions [13]. While DevSecOps and related organizational practices have proven effective for communicating strategic objectives and aligning organizational processes, the aforementioned framework does not entail a systematic abstraction of the biological immune

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

system and a mapping of its core immunological principles, such as innate versus adaptive immunity, humoral versus cellular components, clonal selection, immune memory, or distributed self-/non-self discrimination to corresponding digital counterparts [14]. In general, with the pervasive digitalization of all engineering domains and growing interest in biologically inspired computing principles [15], the term "digital immune system" has been reintroduced and widely propagated as a metaphorical label for existing software engineering practices rather than for biologically inspired architectural concepts in the sense established by decades of research on artificial immune principles and biologically inspired concepts [16].

A review of the digital immune system landscape indicates that across many domains the label "digital immune system" is frequently applied without a biologically explicit functional mapping, while domain-specific concepts for cyber-physical SHM of civil infrastructure remain largely absent. This paper therefore proposes a biologically inspired reference architecture for digital immune systems for civil infrastructure and formally specifies the associated threat categorization at the architecture level. The contribution is conceptual, i.e. selected immune principles are mapped to a layered architecture comprising innate and adaptive layers as well as local modules and global elements for coupled cyber-physical SHM systems, while the threat space addressed by the architecture is expressed through a descriptive formal specification. The architecture is intended to support computational modeling, simulation, and incremental implementation. It does not claim a validated field deployment or a complete algorithmic specification for every module.

The paper is organized as follows. Section 2 reviews the immunological components and processes that motivate the architectural mapping to digital immune systems for civil infrastructure. Section 3 analyzes and formally specifies the threat categories relevant to the proposed reference architecture, presents the reference architecture by assigning selected cellular and humoral components of the biological immune system to local modules and global elements deployable across sensor nodes and central computing resources of the digital immune system, and thereafter introduces an illustrative sensor-fault scenario as a compact architectural instantiation. Furthermore, recommendations for augmenting existing cyber-physical SHM systems with digital immune system functionality are presented from a computational perspective. Section 4 summarizes the main results and outlines potential future research directions.

2 The biological immune system

The biological immune system is a highly coordinated network of cells, tissues, and molecular signals that protect the body from infections and help maintain homeostasis. The biological immune system comprises two interacting immune strategies, *innate immunity*, which provides immediate, broadly acting defense, such as anatomical barriers and pattern recognition receptors that detect conserved pathogen signatures, i.e., pathogen-associated molecular patterns (PAMPs), as well as humoral mediators, such as the complement system and cytokines

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

(soluble mediators), and *adaptive immunity*, which develops more slowly but provides highly specific protection by generating antigen-specific lymphocytes and antibodies. A hallmark of adaptive immunity is immunological memory, enabling rapid and robust responses upon re-exposure, an effect exploited by vaccination. Beyond pathogen control, the immune system contributes to tissue repair and continuously performs immune surveillance of abnormal cells; its regulation is essential, since excessive responses can drive allergies and autoimmune diseases, while insufficient responses increase susceptibility to infections and cancers.

A further distinction can be made between *humoral components*, i.e. soluble factors in body fluids (including antibodies, the complement system, and cytokines) and – in the simplified representation of Fig. 1 – the B-cell lineage (B lymphocytes and memory B cells) as the source of antigen-specific antibodies and humoral immune memory, as well as *cellular components*, mediated by immune cells, with both categories spanning innate and adaptive immunity. Since the biological immune system is extraordinarily complex, the remainder of this section introduces key immune components and processes. The introduction is subdivided into innate and adaptive immunity and is presented in a simplified form from an engineering and computer-science perspective, focusing on the components and processes most relevant to digital immune systems for civil infrastructure. Unless stated otherwise, the term "biological immune system" hereinafter refers to the human immune system. Only components that are subsequently mapped to digital functions in Section 3 are retained; no claim of physiological completeness is made.

The key steps within the biological immune response shown in Fig. 1 are described as follows, introducing immune components with particular relevance to digital immune systems.

- *Step 1*: The *anatomical barriers* (e.g., skin and mucous membranes) form the first level of innate immunity, providing physical protection and preventing a large fraction of pathogens from coming into contact with the cellular and humoral components of the immune system.
- *Step 2*: Pathogens and their conserved molecular patterns that overcome the anatomical barriers are recognized by *pattern recognition receptors* expressed on cells of the innate immune system (2a) and can independently activate the *complement system* (2b), a humoral component, via antibody-independent pathways. The combined recognition activates and amplifies cellular and humoral defense mechanisms and intensifies the ongoing innate immune response.
- *Step 3*: Activation of pattern recognition receptors on *dendritic cells* and *macrophages* brings the cellular components of innate immunity into an activated state. Dendritic cells take up pathogens and their products, extract characteristic features, and process the pathogen-derived material into antigen fragments suitable for presentation to the adaptive immune system, whereas macrophages increase phagocytosis and degradation of the invading pathogen-derived material. In parallel, *natural killer cells* provide a rapid cellular effector mechanism by eliminating infected or stressed host cells, thereby

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

complementing the innate response mediated by the dendritic cells and the macrophages.

- *Step 4*: The dendritic cells form a functional link between innate immunity and adaptive immunity. The dendritic cells present processed antigen fragments to *T lymphocytes* and, in particular, activate *T helper cells*, thereby initiating the adaptive immune response and activating the cellular components of adaptive immunity.
- *Step 5*: The activated T helper cells support and coordinate multiple components within adaptive immunity. *B lymphocytes* are stimulated to produce specific antibodies and to form *memory B cells*. *Memory T cells* arise from a subset of activated effector cells and persist long-term, enabling rapid responses upon re-exposure to the same antigen. In parallel, *cytotoxic T cells* are activated for specific elimination of infected or transformed cells, and *regulatory T cells* are activated and limit the strength of the response to prevent overreactions.
- *Step 6*: The B lymphocytes activated by signals from the T helper cells proliferate and differentiate into cells that produce large quantities of specific *antibodies* against the recognized antigen. A fraction of the activated B lymphocytes differentiates into long-lived memory B cells that store antigen-

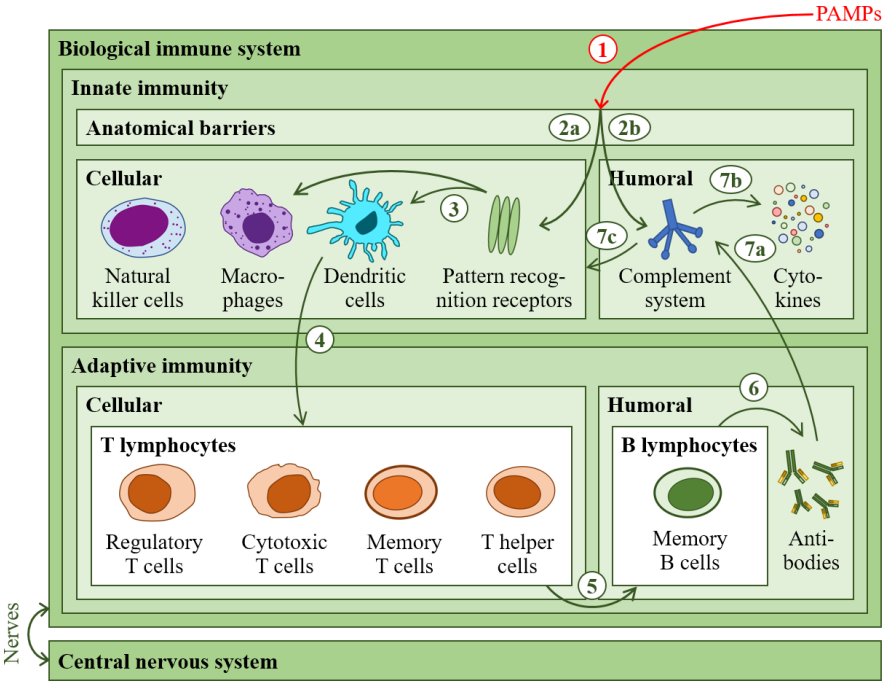

Fig. 1. The biological immune system with selected components and processes relevant to digital immune systems.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

specific information and enable rapid antibody responses upon re-exposure to the same antigen.
- *Step 7*: Antibodies bound to antigen can activate the complement system (7a). Complement activation releases inflammatory mediators that act as regulatory signals and can increase *cytokine* release from activated immune cells (7b). Together, the signals (i.e., complement-derived inflammatory mediators and cytokines) recruit immune cells (in particular macrophages) and enhance additional cellular effector mechanisms (e.g., macrophages and natural killer cells), particularly when antibodies are bound to the target, i.e. the antigen-bearing pathogen or infected/transformed host cell (7c). The interaction of the humoral components (antibodies, complement system, cytokines) and the cellular components (macrophages, natural killer cells) amplifies and focuses the immune response.

To allow the body to coordinate immune responses with nervous-system functions, the immune and nervous systems communicate closely through *nerves* and chemical messengers, such as hormones and neurotransmitters. The *central nervous system* integrates information about the state of the body and can modulate immune responses. Nerves provide communication pathways between peripheral tissues and the central nervous system, thus influencing local immune responses. Antigen recognition, along with innate and adaptive responses, therefore operates within a coordinated framework that links local immune mechanisms to organism-level central regulation. From an engineering perspective, the key implication is not a literal equivalence between immune and nervous systems, but the general principle that local immune processes are coupled to distributed communication pathways and organism-level regulation. This principle motivates the distinction between local modules, communication links, and system-level coordination in Section 3.

3 A reference architecture for digital immune systems for civil infrastructure

This section presents the reference architecture for digital immune systems for civil infrastructure, which is shown in Fig. 2. First, threat categories and requirements are analyzed, and the corresponding threat model is formally specified. Then, the reference architecture is presented, introducing the main modules and elements in a structured functional manner. Next, an illustrative sensor-fault scenario is introduced to demonstrate how selected architectural roles may be instantiated on an existing SHM host platform. Finally, implementation recommendations are formulated, proposed to mature digital immune systems into robust, deployable technology for civil infrastructure.

3.1 Threat categories, requirements analysis, and formal specification

In cyber-physical structural health monitoring of civil infrastructure, the threat landscape is no longer limited to the physical structure alone. As the physical

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

structure and the SHM system form a coupled cyber-physical system, threats can jeopardize the operation of both the physical structure and the SHM system. While internal threats that act on the SHM system are not new (e.g., SHM system faults), the ubiquity of network connectivity introduces an additional category of external threats that manifests itself as cyberattacks. In light of the pace of technological developments, the new threat categories motivate a broader paradigm shift in SHM system design – a new school of thought that treats resilience, trustworthiness, and security as first-class design objectives rather than minor SHM system add-ons. This study therefore considers "health" as a property of coupled cyber-physical SHM systems, not merely as a property describing the physical structure alone, since maintaining trustworthy SHM is inseparable from maintaining structural integrity, and vice versa.

Potential threats may be described from two complementary perspectives. A system-oriented perspective distinguishes between the physical structure and the SHM system, whereas a threat-oriented perspective distinguishes between internal and external sources of disruption. In the present context, "internal" and "external" refer to the coupled system and to the operational scope of the digital immune system, not to the ultimate physical origin of a harmful event. On this basis, the proposed reference architecture addresses three operative threat categories:

- Threat category I (internal): Structural anomalies (including damage) within the physical structure.
- Threat category II (internal): SHM system faults (including sensor faults) within the SHM system.
- Threat category III (external): Cyberattacks (including sabotage) targeting the SHM system.

Combining the system-oriented and threat-oriented perspectives yields, in principle, a two-dimensional classification with four logical cases. The remaining case corresponds to external influences acting directly on the physical structure, namely exogenous physical hazards in a broad sense, including extreme environmental events and deliberate physical attacks, for example explosions. Such hazards are not addressed directly by digital immune functions because the proposed digital immune system operates at the level of sensing, data processing, communication, and system-level response. The remaining case becomes relevant to the digital immune system only when hazards produce observable consequences within the coupled system, for example structural anomalies in the physical structure or impairments within the SHM system. Normal environmental and operational conditions are therefore not treated as threats in themselves, but as part of the operational context. For the sake of logical completeness, the fourth category is retained in the formal specification; however, the operative threat space considered by the reference architecture is restricted to categories I–III.

The threat categories can be expressed formally in a descriptive, architecture-level manner as follows. Let the sorts Threat, Subsystem, Origin, and Category be

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

given. Let

$$\mathsf{PS}, \mathsf{SHM} : \mathsf{Subsystem}, \qquad \mathsf{int}, \mathsf{ext} : \mathsf{Origin}, \qquad \mathsf{I}, \mathsf{II}, \mathsf{III}, \mathsf{IV} : \mathsf{Category}.$$

Assume the basic distinctness conditions

$$\mathsf{PS} \neq \mathsf{SHM} \qquad \text{and} \qquad \mathsf{int} \neq \mathsf{ext},$$

together with

$$\mathsf{I} \neq \mathsf{II} \ \wedge \ \mathsf{I} \neq \mathsf{III} \ \wedge \ \mathsf{I} \neq \mathsf{IV} \\ \wedge \ \mathsf{II} \neq \mathsf{III} \ \wedge \ \mathsf{II} \neq \mathsf{IV} \ \wedge \ \mathsf{III} \neq \mathsf{IV}.$$

To restrict the formalization to the explicitly introduced constants, let the following axioms hold:

$$\forall s : \mathsf{Subsystem} \ \big(s = \mathsf{PS} \vee s = \mathsf{SHM}\big),$$

$$\forall o : \mathsf{Origin} \ \big(o = \mathsf{int} \vee o = \mathsf{ext}\big),$$

$$\forall c : \mathsf{Category} \ \big(c = \mathsf{I} \vee c = \mathsf{II} \vee c = \mathsf{III} \vee c = \mathsf{IV}\big).$$

Let

$$\mathsf{target} : \mathsf{Threat} \to \mathsf{Subsystem} \qquad \text{and} \qquad \mathsf{origin} : \mathsf{Threat} \to \mathsf{Origin}.$$

Exhaustiveness of the case distinction is captured by

$$\forall t : \mathsf{Threat} \ \Big(\big(\mathsf{target}(t) = \mathsf{PS} \vee \mathsf{target}(t) = \mathsf{SHM}\big) \wedge \big(\mathsf{origin}(t) = \mathsf{int} \vee \mathsf{origin}(t) = \mathsf{ext}\big)\Big).$$

Define the categorization function

$$\kappa : \mathsf{Threat} \to \mathsf{Category}$$

by

$$\kappa(t) = \begin{cases} \mathsf{I}, & \text{if } \mathsf{target}(t) = \mathsf{PS} \wedge \mathsf{origin}(t) = \mathsf{int}, \\ \mathsf{II}, & \text{if } \mathsf{target}(t) = \mathsf{SHM} \wedge \mathsf{origin}(t) = \mathsf{int}, \\ \mathsf{III}, & \text{if } \mathsf{target}(t) = \mathsf{SHM} \wedge \mathsf{origin}(t) = \mathsf{ext}, \\ \mathsf{IV}, & \text{if } \mathsf{target}(t) = \mathsf{PS} \wedge \mathsf{origin}(t) = \mathsf{ext}. \end{cases} \tag{1}$$

The threat model defined above therefore provides a formal boundary for the reference architecture and for the architectural mapping developed in the following subsection.

Overall, the formally specified threat categories entail a broadened threat model, and the reference architecture must provide protective capabilities commensurate with the coupled nature of cyber-physical SHM systems as well as with the heterogeneity of the threats. Precisely, the reference architecture must (i) protect and monitor the coupled system comprising the physical structure and the SHM system, rather than treating the SHM system as a neutral observer of the physical structure, (ii) provide explicit coverage of all threat categories –

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

structural anomalies, internal SHM system faults, and external cyberattacks – within one coherent logic, and (iii) integrate rapid, largely non-specific "innate" reactions with slower, threat-specific "adaptive" reactions, enabling early containment alongside targeted diagnosis and mitigation. In addition to capabilities (i)–(iii), the reference architecture must provide (iv) a clear separation between system-level global elements and node-level local modules to support scalable coordination without sacrificing local responsiveness, (v) explicit learning and memory enabling continuous improvement of the detection and response repertoire and reuse of prior experience, and (vi) regulation mechanisms that prevent destabilizing overreactions and enable a controlled return to a normal operating state after a threat has been mitigated. In the remainder of this paper, the reference architecture is discussed against these six requirements at the level of functional design rather than by empirical performance evaluation.

3.2 Core structure, modules, and elements

The reference architecture is designed as a layered framework comprising an *innate layer* and an *adaptive layer*, functionally analogous to innate and adaptive immunity in the biological immune system. The innate layer ensures rapid, largely non-specific responses to threats, whereas the adaptive layer provides more specific and regulated responses. Each layer comprises *local modules* with node-level scope and *global elements* with system-level scope, functionally reflecting cellular and humoral immune roles, respectively. Therein, the B-cell lineage is treated as humoral-oriented because it generates and maintains the system-wide repertoire of soluble effectors (antibodies). The local modules implement functional roles executed close to data sources and may run on stationary sensor nodes attached to the physical structure, on mobile sensor nodes (e.g. following the concept of mobile robotics, as proposed in [17]), or on a *central server*, which provides system-level coordination. The global elements may either reside at the aforementioned locations or be assembled on demand at runtime and migrate between computing locations, as demonstrated in [18]. *Communication links* interconnect all system entities. The mapping is therefore functional and architectural rather than literal or physiological. The entities are introduced as follows, organized along the key steps within the response process.

- *Step 1*: The *physical protection* (equivalent to anatomical barriers in the biological immune system) in the form of *coatings* and *sealants* (equivalent to skin and mucous membranes) constitutes the first level of the innate layer for the coupled system of physical structure and SHM system.
- *Step 2*: Threats that overcome physical protection are recognized within the innate layer by the *sensing modules* (equivalent to pattern recognition receptors) and can independently activate the *amplification logic* (equivalent to the complement system). Together, the dual recognition activates and amplifies the innate local and global defense in the digital immune system.
- *Step 3*: Activation of the sensing modules causes the *feature processing modules* (equivalent to dendritic cells) and the *non-specific diagnostic modules*

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

(equivalent to macrophages) to become active. Feature processing extracts features from suspicious data fragments and prepares identified threat patterns for transfer to the adaptive layer, while non-specific diagnostics locally examine structural and system data for anomalies. In parallel, the *threat containment modules* (equivalent to natural killer cells) provide a rapid cellular effector mechanism by isolating compromised system entities and restricting suspicious communication endpoints, thereby complementing the innate responses mediated by feature processing and non-specific diagnostics. Herein, feature processing is understood as the transformation of raw measurements, metadata, and communication events into compact threat-relevant representations for decision-making.

- *Step 4*: The feature processing modules assume the above-mentioned mediating role between the innate layer and the adaptive layer. The processed feature representations of threat patterns are transmitted via communication links to the *adaptive response modules* (equivalent to T lymphocytes) and activate, in particular, the *response orchestration modules* (equivalent to T helper cells), i.e. the adaptive layer of the digital immune system is activated, and the adaptive response is initiated.
- *Step 5*: The response orchestration modules assume the central coordination function within the adaptive response modules. At this stage, the adaptive layer evaluates whether the observed pattern is consistent with expected system behavior ("self") or indicates a harmful deviation ("non-self"), thereby constraining the set of admissible responses. *Learners* (equivalent to B lymphocytes) are triggered to generate *markers* (equivalent to antibodies) and to update the *threat signature memory* (equivalent to memory B cells). The *intervention memory modules* (equivalent to memory T cells) store successful response sequences for recurring threats, the *threat neutralization modules* (equivalent to cytotoxic T cells) are activated for specific shutdown or isolation of compromised components, and the *response regulation modules* (equivalent to regulatory T cells) limit reaction strength and prevent harmful overreactions.
- *Step 6*: Activated learners generate a repertoire of specific markers (equivalent to antibodies) in the form of digital signatures, models, or decision rules for the identified threat pattern based on information provided by response orchestration. At the same time, a fraction of the generated markers is stored as new entries in the threat signature memory, enabling fast and reliable recognition of recurring threats in the future.
- *Step 7*: Markers bound to specific threat patterns activate the amplification logic as part of the global elements (7a). Activated amplification logic generates additional *regulatory signals* (equivalent to cytokines) (7b) and stimulates the non-specific diagnostic modules to intensify inspection and direct the local modules toward affected data and system areas (7c). In parallel, the threat containment modules are directed toward suspicious system entities for restriction or isolation. The coordinated interaction of markers, amplification logic, and regulatory signals (at the global level) with non-specific diagnostics

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

and threat containment (at the local level) amplifies and focuses the digital immune system response.

3.3 Illustrative use-case scenario: Sensor-fault diagnosis

To complement the reference architecture without turning the paper into a system-specific implementation study, a compact illustrative sensor-fault scenario is introduced in the following. The use-case scenario is intended to demonstrate how selected architectural roles may be instantiated on an existing SHM host platform under a representative fault condition. The use-case scenario therefore serves to illustrate operational plausibility rather than to report a validated digital immune system implementation.

The use-case scenario is grounded in an existing wireless SHM setup with multiple sensor nodes and a central computing unit (CCU). A representative bias fault (threat category II) affecting one acceleration channel is considered. Within the present terminology, an "innate sensor node" denotes a sensor node that hosts local modules of the innate layer, i.e. sensing, non-specific diagnostics, feature processing, and threat containment. An "adaptive sensor node" denotes a sensor node that hosts local modules of the adaptive layer, i.e. adaptive response functions centered on response orchestration. The CCU is understood here as part of the SHM system rather than as an external entity, providing system-level computing, data management, and coordination within the coupled cyber-physical SHM system. System-level functions of the digital immune system, including amplification logic, regulatory signals, markers, learners, and threat signature memory, may reside at the CCU and support the local modules from there. In addition, the proposed architecture permits selected software functions to migrate

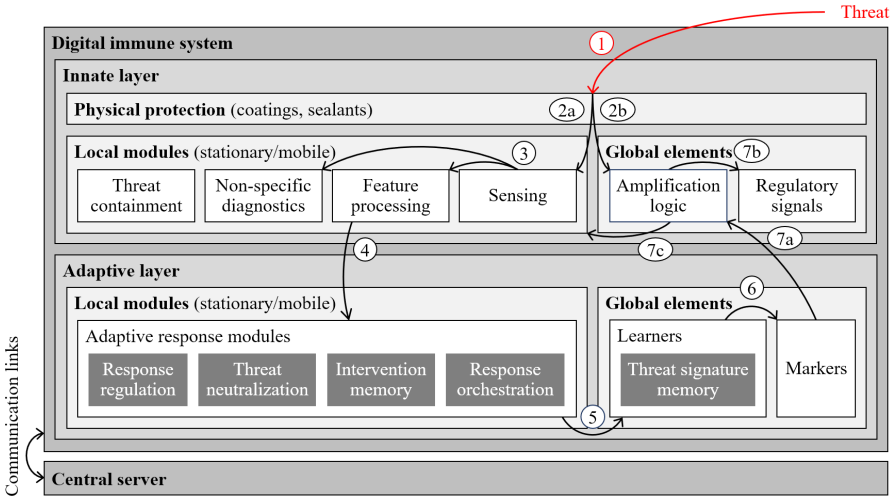

Fig. 2. Reference architecture for digital immune systems.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

between sensor nodes and the CCU if current diagnostic demands or resource constraints require a specific allocation of computational tasks. The distinction between innate and adaptive sensor nodes is therefore functional rather than hardware-inherent and merely serves to illustrate one admissible deployment pattern of the reference architecture.

Figure 3 outlines a representative interaction sequence for the bias-fault scenario, including the corresponding key steps of the process, as described in Section 3.2. Once the abnormal sensor stream becomes observable, the sensing module on the innate sensor node recognizes a suspicious pattern and may, in parallel, trigger system-level amplification logic on the CCU. The resulting alert activates non-specific diagnostics and feature processing on the same node, where compact fault-relevant descriptors are derived from the abnormal measurements. The feature representation is then transferred to the adaptive sensor node, where response orchestration initiates a more specific diagnosis and, if needed, requests additional support from learners and previously stored markers at the CCU level. Where required, selected adaptive functions may be migrated temporarily from the CCU to the adaptive sensor node, or vice versa, so that specialized analysis can be executed at the most suitable location within the SHM system. Depending on the available evidence, a known fault pattern may be matched directly, whereas an unfamiliar pattern may lead to marker refinement or marker generation under regulated conditions. Once the fault has been sufficiently confirmed, the adaptive diagnosis feeds back into system-level coordination: Amplification logic and regulatory signals guide the local response, threat containment limits the influence of the faulty channel, and stronger actions remain available only if required. As a result, the use-case scenario illustrates a progression from rapid local screening to more specific adaptive interpretation and regulated response across sensor nodes and the CCU as constituent parts of the SHM system.

3.4 Implementation recommendations

Translating the conceptual reference architecture into field-deployable technology for civil infrastructure requires both protective effectiveness and well-regulated response behavior, since an inadequately calibrated digital immune system may overreact to benign operational variability, environmental fluctuations, or gradual aging and cause false alarms, unnecessary isolation of system entities, or disruptive interventions. The main priorities are therefore to strengthen immune-process modeling and analysis, align fault diagnosis and cybersecurity methods with SHM-specific requirements and the innate-adaptive distinction, prioritize realistic, large-scale simulations in cyber-physical SHM environments, develop modular deployment strategies exploiting parallel and distributed computing, edge-cloud integration, and runtime migration where beneficial, and establish open reference implementations and benchmarks. At the same time, the paper does not provide a validated implementation or a module-level algorithmic specification, but instead offers a domain-specific architectural basis that can be instantiated incrementally, beginning with a small set of innate local modules and subsequently extending toward adaptive-layer capabilities as validation evidence accumulates.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

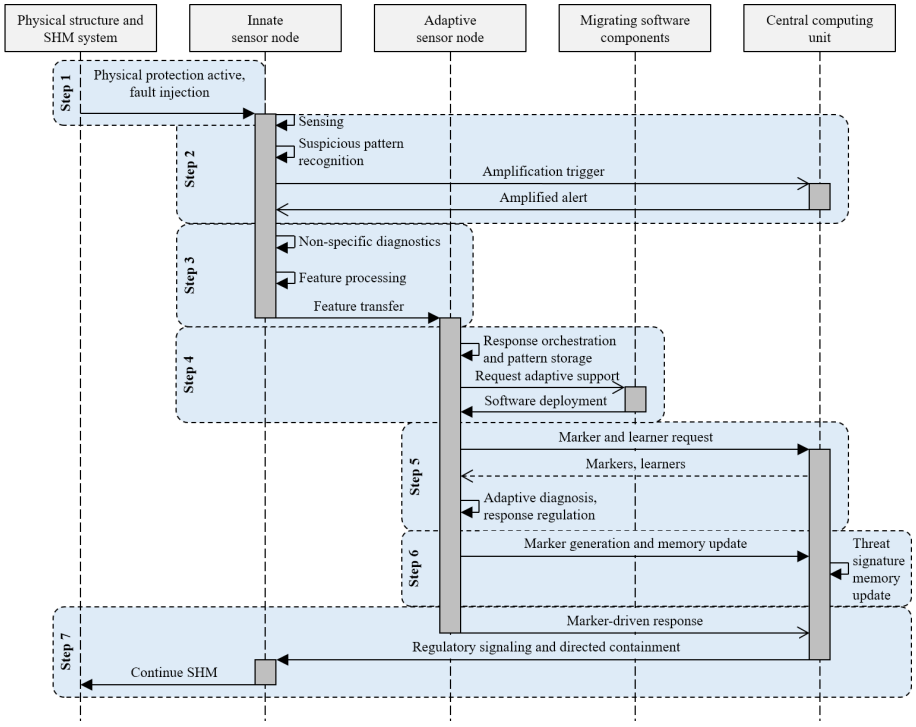

Fig. 3. Interaction sequence for the use-case scenario.

4 Summary and conclusions

With the ongoing digital transformation of civil infrastructure, structural health monitoring has evolved toward coupled cyber-physical systems in which the physical structure and the SHM system must be protected as a whole, since the relevant threat space extends beyond structural anomalies and internal SHM system faults to include external cyberattacks. To address the broadened threat landscape, this paper has proposed a biologically inspired, computing-oriented reference architecture for digital immune systems for civil infrastructure. In contrast to existing uses of the term "digital immune system", which either target other domains or lack a systematic biological mapping, the proposed architecture builds on an explicit and biologically grounded mapping of immune functions to digital counterparts, combines a system-oriented threat categorization with a descriptive formal specification of the threat space, organizes the digital immune system into innate and adaptive layers with local modules and global elements, and is complemented by an illustrative sensor-fault scenario that demonstrates how selected architectural roles may be instantiated on realistic SHM components. Future work should determine to what extent the proposed architecture can be operationalized, validated, and resource-efficiently deployed in realistic cyber-physical SHM settings.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

Acknowledgments. This study is thematically aligned with research projects funded by the German Research Foundation (DFG) under grants SM 281/9-3, SM 281/22-1, SM 281/30-1, SM 281/31-1, SM 281/32-1, SM 281/33-1, SM 281/41-1, SM 281/44-1, and GRK 3068 as well as by the German Federal Ministry of Transport (BMV) under grant 01FV2059C. The financial support provided by DFG and BMV is gratefully acknowledged. Furthermore, the author would like to thank Kosmas Dragos (Hamburg University of Technology, Germany) for providing valuable technical expertise. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author and do not necessarily reflect the views of the aforementioned sponsors or individuals.

Disclosure of Interests. The author has no competing interests to declare that are relevant to the content of this article.

References

1. Sohn, H., Farrar, C. R., Hemez, F. M., and Czarnecki, J. J. (2002). A review of structural health monitoring literature: 1996–2001. Los Alamos National Laboratory Report LA-13976-MS, Los Alamos, NM, USA.
2. Lynch, J. P., & Loh, K. J. (2006). A summary review of wireless sensors and sensor networks for structural health monitoring. Shock and Vibration Digest, 38(2), 91–128.
3. Worden, K. & Manson, G. (2007). The application of machine learning to structural health monitoring. Philosophical Transactions of the Royal Society A, 365(1851), 515–537.
4. Al-Nasser, H., Al-Zuriqat, T., Dragos, K., Chillón Geck, C., & Smarsly, K. (2024). Identification of combined sensor faults in structural health monitoring systems. Smart Materials and Structures, 33(8), 085026.
5. Fitz, T., Theiler, M., & Smarsly, K. (2019). A metamodel for cyber-physical systems. Advanced Engineering Informatics, 41, 100930.
6. Al-Zuriqat, T., Chillón Geck, C., Dragos, K., & Smarsly, K. (2023). Adaptive fault diagnosis for simultaneous sensor faults in structural health monitoring systems. Infrastructures, 8(3), 39.
7. Kephart, J. O., Sorkin, G. B., & Swimmer, M. (1997). An immune system for cyberspace. In: Proceedings of the 1997 IEEE International Conference on Systems, Man, and Cybernetics: Computational Cybernetics and Simulation (Vol. 1, pp. 879–884), Orlando, FL, USA, October 12–15, 1997.
8. Soltani Halvaiee, N. & Akbari, M. (2014). A novel model for credit card fraud detection using artificial immune systems. Applied Soft Computing, 24, 40–49.
9. He, J., Li, T., Li, B., Lan, X., Li, Z., & Wang, Y. (2021). An immune-based risk assessment method for digital virtual assets. Computers & Security, 102, Article 102134.
10. Lakhotia, P., Dwivedi, R., Sharma, D. K., & Sharma, N. (2023). Intrusion detection system for IoE-based medical networks. Journal of Database Management, 34(2), 1–18.
11. Hosseini, S., Seilani, H., Heidary, M., & Hwang, Y.-S. (2025). Artificial immune systems for industrial intrusion detection: A systematic review and conceptual framework. Journal of Engineering, 2025, Article ID 8408209.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10

12. Falowo, O. I., Botsyoe, L. E., Koshoedo, K., & Ozer, M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access, 12, 123811–123822.
13. Gartner, Inc. (2022). What Is a Digital Immune System and Why Does It Matter? Gartner Technical Insight, Stamford, CT, USA. Accessed December 24, 2025. Available at: https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter.
14. Hofmeyr, S. A. & Forrest, S. (2000). Architecture for an artificial immune system. Evolutionary Computation, 8(4), 443–473.
15. Fritz, H. & Smarsly, K. (2020). A state-of-the-art review of nature-inspired systems for smart structures. In: Proceedings of the European Workshop on Structural Health Monitoring (EWSHM), Palermo, Italy, July 4-7, 2020.
16. Dasgupta, D., Yu, S., & Majumdar, N. (2005). MILA—Multilevel immune learning algorithm and its application to anomaly detection. Soft Computing, 9(3), 172–184.
17. Smarsly, K., Dragos, K., Stührenberg, J., & Worm, M. (2023). Mobile structural health monitoring based on legged robots. Infrastructures, 8(9), 136.
18. Smarsly, K. & Law, K. H. (2013). A migration-based approach towards resource-efficient wireless structural health monitoring. Advanced Engineering Informatics, 27(4), 625–635.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29909-3_10