

Transport and Telecommunication, 2026, volume 27, no. 3, 297-308
Transport and Telecommunication Institute, Lauvas 2, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2026-0022

THE TELEMATICS-ENABLED COORDINATION OF MOBILE EMERGENCY DECONTAMINATION PROCESSES IN TRANSPORT HUBS

Deniss Bičkovs¹, Sergejs Borzihs², Veranika Khlud³

^{1,2} Arete Technologies

Riga, Latvia, Ezera iela 35, LV-1034

³ Riga Technical University

Riga, Latvia, Kipsalas Street 6a, LV-1048

¹deniss.bickovs@gmail.com, ²sb@arete-tech.com, ³sb@arete-tech.com

Mass decontamination in transport hubs is a time-critical emergency-response task following accidents involving hazardous goods, where operational effectiveness depends on rapid coordination, reliable control, and traceable execution. This paper proposes a telematics-enabled digital coordination framework for mobile emergency decontamination in transport-hub environments. The framework is formalised as a four-layer cyber-physical architecture integrating operator interaction, application-layer control, equipment-level execution, and persistent audit-oriented data management. Its operational logic is supported by a deterministic lifecycle model, algebraic preset validation, and role-based access control. The proposed approach was evaluated through scenario-based simulation and a transport-hub case study. The results confirmed functional correctness and operational feasibility of the framework, while the case study indicated a 42% reduction in mean response time and a 44% reduction in sustainability-related operational loss compared with conventional manual coordination. The study shows that mobile decontamination can be interpreted as a digitally coordinated safety service within transport hubs and that telematics-enabled orchestration can improve response readiness and operational resilience in disruption-sensitive environments.

Keywords: Transport hubs, hazardous goods, mobile decontamination, telematics, cyber-physical systems, emergency response, transport resilience

1. Introduction

Mass decontamination of persons exposed to chemical, biological, radiological, or nuclear (CBRN) agents is one of the most demanding tasks in emergency response. In transport hubs such as ports, airports, railway terminals, and logistics nodes, this challenge becomes especially acute because hazardous exposure may propagate through interconnected operational zones, disrupt cargo and passenger flows, and compromise service continuity beyond the initial incident area. In such environments, response effectiveness depends not only on the physical availability of decontamination equipment, but also on the speed, coordination, traceability, and reliability of operational control.

In many existing deployment settings, mobile decontamination processes are still coordinated manually. Equipment configuration, process initiation, communication between responders, and post-event registration are often managed through fragmented procedures and operator-dependent actions. Under time pressure, these arrangements increase the risk of delay, inconsistency, and human error. From the perspective of transport telematics, this means that mobile decontamination remains weakly integrated into the digital coordination environment of the transport hub, despite the growing role of connected control, cyber-physical integration, and resilience-oriented operational management in modern transport systems.

This observation suggests that mobile decontamination in transport hubs should be interpreted not merely as an isolated emergency device, but as a digitally coordinated safety service embedded in a wider transport-hub information and control environment. Such a perspective shifts attention from the equipment itself to the underlying coordination logic, including lifecycle control, parameter consistency, access-governed operation, communication latency, and auditability. It also creates a basis for evaluating emergency-response performance in terms relevant to transport systems, such as response readiness, disruption containment, and operational resilience.

This paper addresses the problem by proposing a telematics-enabled digital coordination framework for mobile emergency decontamination in transport-hub environments. The framework is formalised as a four-layer cyber-physical architecture integrating operator interaction, application-layer control, equipment-level execution, and persistent audit-oriented data management. Its operational logic is further supported by a deterministic lifecycle model, algebraic preset validation, and role-based access control. The proposed approach is evaluated through scenario-based simulation and a transport-hub case study in order to assess both functional feasibility and operational relevance.

The remainder of the paper is organized as follows. Section 2 reviews the relevant literature and identifies the research gap. Sections 3–5 present the proposed framework, its formal model, requirements, and prototype implementation. Section 6 reports the simulation-based validation results, Section 7 presents the transport-hub case study, and Section 8 concludes the paper.

2. Related works

The literature relevant to this study may be grouped into three closely related streams: research on mass-casualty decontamination and emergency-response operations, studies of transport-hub resilience and cyber-physical coordination, and methodological work on scenario-based validation of safety-critical systems. Taken together, these streams establish the operational importance of the problem and clarify the specific gap addressed in this paper.

The first stream concerns mass-casualty decontamination and emergency-response management. Prior studies have shown that the effectiveness of decontamination depends not only on equipment availability, but also on operational timing, responder communication, process consistency, and documentation quality (Levitin *et al.*, 2003; Chilcott, 2014; Cibulsky *et al.*, 2015; Collins *et al.*, 2021). Large-scale exercise studies further demonstrate that coordination failures often arise in resource allocation, process timing, and multi-agency interaction, while communication quality significantly affects both operational efficiency and user compliance (Currie and Heslop, 2018; Dennis *et al.*, 2023; Carter *et al.*, 2012; Carter *et al.*, 2014; Carter and Amlôt, 2016). This body of work shows that decontamination is a system-level coordination problem rather than a purely technical equipment task.

The second stream relates to transport systems, transport-hub resilience, and intelligent cyber-physical coordination. Recent work has emphasised that transport hubs are disruption-sensitive infrastructures in which safety, continuity of operations, and resilience increasingly depend on connected sensing, information exchange, and coordinated control (Ahmed and Dey, 2020; Zhang *et al.*, 2023; O’Kelly, 2025; Avcı and Koca, 2024; Pavão *et al.*, 2024; Aslam *et al.*, 2025). This perspective is directly relevant to emergency decontamination in ports, airports, railway terminals, and logistics nodes, where delayed response may propagate operational disruption beyond the initial hazardous zone. However, the existing transport-oriented literature pays limited attention to mobile decontamination as a digitally coordinated transport-hub safety service.

The third stream is methodological. In safety-critical cyber-physical domains, scenario-based validation and simulation are widely used where full-scale real-world experimentation is costly, risky, or impractical. Prior studies stress that meaningful virtual evaluation requires explicit scenario selection, model validity, and traceable verification logic (Riedmaier *et al.*, 2021; Lee *et al.*, 2023; Wiśniewski *et al.*, 2019). This methodological position is directly applicable to mobile emergency decontamination, where realistic validation must be combined with operational safety and controlled testability.

Despite these advances, three gaps remain. First, the literature does not provide a transport-hub-oriented telematics framework for mobile decontamination that treats the process as a digitally coordinated safety service rather than as a standalone emergency device. Second, existing studies do not offer a unified formal model combining lifecycle control, parameter consistency, and access-governed operation for this class of system. Third, quantitative evidence remains limited regarding the operational effect of such digital coordination on response readiness in realistic transport-hub emergency scenarios.

This paper addresses these gaps by proposing and evaluating a telematics-enabled digital coordination framework for mobile emergency decontamination in transport-hub environments. Unlike prior studies that examine decontamination primarily as an operational or procedural response task, the present study conceptualises it as a digitally coordinated cyber-physical safety service embedded in the information and control environment of a transport hub. The main contributions are fourfold: (1) the paper formulates a transport-hub-oriented coordination model for mobile decontamination as a cyber-physical safety service; (2) it formalises lifecycle control, preset validation, and role-based operational access within a unified framework; (3) it establishes a traceable scenario-based validation approach for this class of systems; and (4) it quantifies the operational relevance of the proposed approach through a transport-hub case study and comparative simulation against manual coordination.

3. System architecture and formal model

To address the identified gap, this study develops a telematics-enabled digital coordination framework for mobile emergency decontamination in transport-hub environments. The framework is conceived as a cyber-physical safety-service model integrating operator interaction, application-layer coordination, equipment-level execution, and persistent audit-oriented data management. Such

formalisation is important because emergency deployment in transport hubs must be coordinated under time pressure, infrastructure constraints, and multi-actor operational dependencies, while maintaining reliable control and traceable execution (Stouffer *et al.*, 2011; Vyatkin, 2013).

The framework is structured as a four-layer architecture formally defined as the tuple

$$\mathcal{G} = \langle \mathcal{L}, \mathcal{C}, \mathcal{D} \rangle,$$

where $\mathcal{L} = \{L_1, L_2, L_3, L_4\}$ denotes the layer set, $\mathcal{C}$ is the inter-layer communication protocol set, and $\mathcal{D}$ is the persistent data store. The four layers correspond to the operator interface, application logic, equipment interaction, and data persistence, respectively. Every state-changing request traverses the layers sequentially and is recorded in $\mathcal{D}$, ensuring coordination traceability and post-event auditability. Figure 1 illustrates the proposed architecture and the corresponding inter-layer information flows.

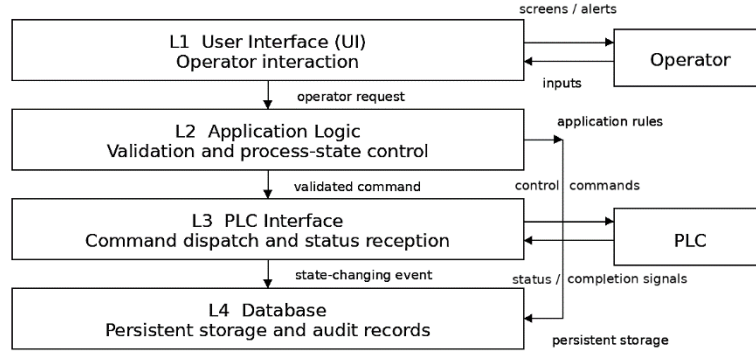


Figure 1. Four-layer architecture of the proposed telematics-enabled coordination framework

The process lifecycle is modelled as a deterministic finite automaton

$$M = (S, \Sigma, \delta, s_0, F),$$

where S is the state set, Σ is the input alphabet, δ is the transition function, s_0 is the initial state, and F is the set of admissible completion states (Cassandras and Lafortune, 2008; Holloway and Butler, 1996). The model captures the lifecycle of a mobile decontamination process from configuration and readiness to execution, interruption, emergency stop, and controlled completion. Undefined inputs are rejected and logged, ensuring that no unspecified operator action may produce an uncontrolled system state. In particular, the emergency state is reachable from active operational states via an abort action, while return from emergency requires an explicit reset, preventing inadvertent restart.

To guarantee process consistency before execution, every configuration preset p is subject to a validity predicate

$$\mathcal{V}(p) = 1$$

only if the hot-water, cold-water, and total-fluid parameters satisfy the predefined balance and admissibility constraints. This algebraic validation prevents inconsistent parameter combinations from being transmitted to the equipment layer and provides a deterministic precondition for safe process initiation. After execution, the deviation between configured and actual fluid volume is recorded as a control variable for process assessment and traceability.

Operational access is governed through role-based control. Let R denote the role set and U the user set, with role assignment defined by $UA \subseteq U \times R$. Access to operation o is permitted only if the corresponding permission predicate

$$\Pi(u, o) = 1$$

holds for the given user-role assignment and the authorised role subset (Sandhu *et al.*, 1996; Ferraiolo *et al.*, 2001). This mechanism ensures that safety-critical operations, including process initiation, interruption, reset, and record modification, remain access-governed and auditable throughout the lifecycle.

Because transport-hub emergency response is highly time-sensitive, the framework additionally imposes a latency constraint on equipment-level command transfer

$$L \leq L_{\max},$$

where $L_{\max} = 200\text{ms}$ is the admissible upper bound. This condition ensures that digital coordination remains compatible with operational response requirements and supports deterministic command execution

under deployment conditions. Measurements obtained from the implemented prototype yielded $L_{99} = 71\text{ms}$ over 200 transactions, providing a compliance margin of 129 ms with respect to the required limit.

Taken together, the proposed framework combines architectural decomposition, deterministic lifecycle control, algebraic configuration validation, access-governed operation, and latency-bounded execution in a unified formal model. Although developed for mobile emergency decontamination, the model can be interpreted more broadly as a coordination logic for digitally managed mobile safety services operating in transport-node environments.

4. Functional and non-functional requirements

The proposed framework is specified through a structured set of functional and non-functional requirements derived from expert consultations in civil protection and subsequently refined through prototype-oriented design feedback. In total, the specification comprises 15 functional requirements and 20 non-functional requirements. The functional requirements cover three principal capability groups: configuration of process presets, registration and retrieval of person-related records, and lifecycle management of decontamination processes. The non-functional requirements address five quality dimensions: reliability, security, equipment interoperability, data integrity, and usability. The complete requirement set is summarised in Appendix A.

At the functional level, the specification enforces several key coordination constraints. First, each configuration preset must satisfy the consistency condition imposed by the validity predicate $\mathcal{V}(p) = 1$, ensuring that fluid-related process parameters are admissible before execution. Second, person-related records must satisfy uniqueness and retrieval constraints in order to support reliable identification and post-event traceability. Third, process execution is governed by strict preconditions: a decontamination process may enter the active state only if both a valid preset and an associated person record have been assigned. Fourth, completion of the process automatically generates execution-related records and locks the resulting process entry against further modification. Together, these constraints ensure that process initiation, execution, and closure remain deterministic, traceable, and formally governed.

At the non-functional level, the requirements ensure that the framework is suitable for safety-critical deployment in transport-hub environments. Reliability requirements address availability, recovery after communication disruption, and loss-free processing of operational data. Security requirements cover role-based access enforcement, server-side validation, and immutable audit logging. Interoperability requirements impose timing and communication constraints on equipment-level command exchange, including the admissible upper latency bound $L_{\max} = 200\text{ms}$. Data-oriented requirements ensure schema-level consistency, referential integrity, and read-only preservation of completed process records. Usability requirements constrain the number of interaction steps for primary actions and require consistent, unambiguous operator feedback.

To support systematic verification, the requirements are organised in a traceability structure linking functional constraints to use cases, validation scenarios, and related non-functional properties. This structure ensures that each major operational function is grounded in a corresponding interaction scenario and can be assessed through explicit validation logic rather than informal inspection. In this sense, the requirement model serves not only as a design specification, but also as a bridge between the formal coordination framework presented in Section 3 and the simulation-based validation reported in Section 6.

5. Prototype implementation

The proposed framework was implemented as a prototype integrating the four functional layers introduced in Section 3. The implementation combines a web-based operator interface, an application server responsible for lifecycle control and access-governed operation, an equipment communication layer, and a persistent relational data store. In this way, the prototype realises the proposed coordination logic as an operational cyber-physical system rather than as a purely conceptual model.

At the execution level, the prototype supports bidirectional interaction with the mobile safety equipment through a dedicated control interface and a serial communication protocol. At the application level, the system enforces the lifecycle model M and evaluates the permission predicate $\Pi(u, o)$ on every protected operation. State transitions and audit-log entries are committed within a single transactional logic, ensuring consistency between process control and persistence. If communication with the equipment fails, the command is retried once within a bounded interval; repeated failure triggers a fault notification in accordance with the interoperability requirements.

The persistence layer is implemented as a relational schema covering users, roles, presets, person-related records, process records, and audit events. To preserve post-execution integrity, completed or aborted process entries are automatically marked as read-only at the database level, independently of the application interface. This design ensures that the traceability constraints defined in Section 4 are enforced not only procedurally but also structurally.

The prototype was deployed in a single-server configuration and used as the implementation basis for the validation campaign reported in Section 6. Measurements of equipment-level command transmission over 200 transactions yielded $L_{99} = 71\text{ms}$, which remained within the admissible latency bound of 200 ms and provided a compliance margin of 129 ms. Figure 2 presents the histogram of equipment-level command latency relative to the admissible threshold $L_{\max} = 200\text{ms}$. These results confirm that the proposed framework is not only formally specified, but also implementable in a form compatible with time-sensitive emergency-response coordination.

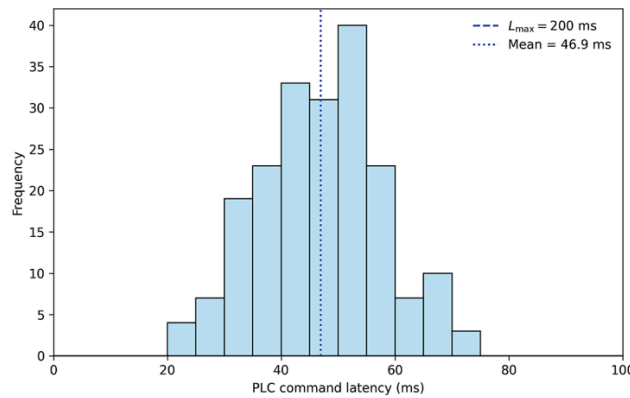


Figure 2. Histogram of equipment-level command latency measurements

6. Simulation-based validation and test results

Validation was conducted in a simulated environment representing emergency-response conditions relevant to CBRN deployment contexts. The evaluation comprised 18 structured scenarios grouped into five validation dimensions: functional correctness, equipment communication and interoperability, multi-scenario operational stability, operator usability, and data integrity with access control. Each scenario followed the Given–When–Then logic in order to ensure explicit and reproducible pass/fail conditions. The complete scenario specifications are provided in Appendix B.

Four aggregate metrics were used to assess the prototype: scenario pass rate, defect severity, data integrity index, and non-functional compliance index. The acceptance thresholds were defined as a scenario pass rate of at least 90%, zero critical defects, data integrity of at least 99%, and non-functional compliance of at least 85%.

The validation results confirmed full functional feasibility of the proposed framework. All 18 scenarios were completed successfully, yielding a 100% pass rate and no critical or major defects. Functional correctness was confirmed for the full process lifecycle, preset consistency enforcement, role-based access restrictions, and automated process completion logic. Equipment interoperability tests showed stable command exchange and compliance with the timing requirement, with latency measurements of $\bar{L} = 47\text{ms}$, $\sigma = 12\text{ms}$, and $L_{99} = 71\text{ms}$, all remaining within the admissible upper bound of 200 ms. Communication fault injection was detected within 1.1 s, satisfying the corresponding notification requirement.

Operational stability was additionally confirmed under extended and concurrent execution conditions. During a sustained 30-minute run, 3,600 sensor readings were processed without data loss. Concurrent sessions preserved independent process-state evolution, while injected anomalies generated the expected alerts without producing uncontrolled transitions. Emergency abort remained executable within 340 ms. Usability testing showed that operators were able to complete the required workflow without exceeding the prescribed navigation constraints, and all primary status messages were judged understandable during the evaluation. The observed usability issues were minor and did not affect functional correctness.

Data integrity and access control requirements were also satisfied. Restricted operations were consistently blocked and logged, referential integrity was enforced at the database level, and all state-

changing actions were recorded together with user identity, timestamp, and execution outcome. As a result, the data integrity index reached 100%. The overall non-functional compliance index was 95%, exceeding the predefined acceptance threshold. The single partial-compliance item concerns full GDPR-scope data protection, including encryption at rest, anonymisation support, and data-subject request handling, which remains planned for the post-prototype phase and does not affect the operational validity of the current framework.

Taken together, the validation results show that the proposed coordination framework is functionally correct, operationally stable, and technically feasible under simulated emergency-response conditions.

7. Case study. Port deployment scenario

7.1. Operational context and motivation

The transport-hub case study examines the deployment of the proposed framework in a hazardous-cargo port environment, where emergency response must be coordinated under conditions of high operational density, elevated escalation risk, and strict continuity requirements. In such settings, delayed or poorly coordinated decontamination may extend the affected area beyond the initial incident zone, disrupt adjacent cargo-handling processes, and reduce the operational resilience of the hub as a whole. The case therefore interprets mobile emergency decontamination not as an isolated technical intervention, but as a digitally coordinated safety service embedded in the operational logic of the transport node.

Formally, the port-zone deployment context may be characterised as a hazardous operational state determined by the type of cargo involved, the local density of activity and personnel, and the risk of incident propagation beyond the initial area. Under such conditions, response readiness, local containment, and traceable execution become critical system-level requirements rather than secondary operational attributes. Figure 3 illustrates the mobile safety installation used as the implementation basis for the case study.



Figure 3. Mobile safety installation used as the implementation basis for the port deployment case study

7.2. Scenario definition and system mapping

Two response configurations are considered. In Scenario A, response coordination relies on manual decision-making, sequential dispatch communication, and non-integrated on-site setup. In Scenario B, the proposed framework supports digitally coordinated deployment through preconfigured process presets, reduced preparation time, and direct transfer of execution parameters to the equipment layer. The essential structural difference between the two scenarios lies not only in equipment availability, but in the replacement of fragmented coordination logic by platform-supported operational orchestration.

From a transport-systems perspective, this difference is significant because emergency-response performance in a hub depends on how rapidly a safety service can be mobilised, configured, and brought to operational readiness without introducing additional coordination delay. The integrated scenario therefore represents a telematics-enabled reduction of response latency rather than merely a local automation improvement.

7.3. Response time model and Monte Carlo simulation

The total response time from hazardous event detection to operational readiness is represented as the sum of five components: incident detection and confirmation, decision and dispatch, mobilisation and movement, local preparation, and initiation of the first controlled safety cycle. Each component is modelled as a triangular random variable defined by minimum, most likely, and maximum values

$$T_x \sim \text{Tri}(a_x, m_x, b_x),$$

where a_x , m_x , b_x are the minimum, mode, and maximum values. This distribution was selected as an appropriate approximation for scenario-based emergency modelling under limited-data conditions, because it enables bounded representation of expert-informed response intervals while preserving interpretability for comparative simulation.

The adopted parameters for both scenarios are given in Table 1.

Table 1. Input parameters of the response time model (minutes)

Component	Meaning	Scenario A — Conventional $\text{Tri}(a_x, m_x, b_x)$	Scenario B — Arete Logic $\text{Tri}(a_x, m_x, b_x)$
T_{det}	Detection and confirmation	(3, 5, 8)	(2, 3, 5)
T_{dec}	Decision and dispatch	(5, 8, 15)	(1, 2, 4)
T_{mob}	Mobilisation / movement	(10, 18, 30)	(6, 10, 16)
T_{setup}	Local preparation	(8, 12, 20)	(4, 6, 10)
T_{start}	First cycle initiation	(2, 4, 6)	(1, 2, 3)

In the conventional scenario, wider distributions reflect dependence on manual coordination and non-dedicated resources. In the integrated scenario, the reduced distributions reflect the effect of platform-level orchestration, preset-based configuration, and automated command transfer. A Monte Carlo simulation with 10,000 runs was performed for each scenario in order to estimate expected deployment time and relative operational improvement.

The results show that the proposed framework reduces the mean time to operational readiness from 47.3 min to 27.4 min, corresponding to a relative improvement of 42%. For disruption-sensitive port environments, this reduction is operationally significant because it shortens the interval during which hazardous exposure may propagate across adjacent operational areas. From a transport-telematics perspective, the result indicates that digitally coordinated safety-service deployment can contribute directly to hub resilience by limiting delay amplification and improving the speed of local response restoration. Table 2 summarises the simulation results.

Table 2. Simulation results — response deployment time

Scenario	Mean response time (min)	Normalised value	Relative improvement
A: Conventional response	47.3	1.00	—
B: Arete Logic integrated	27.4	0.58	42%

To assess the robustness of this effect, a one-factor sensitivity analysis was performed using the deployment delay ratio and the effectiveness of platform-level orchestration as the principal parameters. Figure 4 shows the resulting family of curves. The analysis confirms that the relative advantage of the integrated scenario remains directionally stable across different deployment conditions, although the magnitude of improvement depends on the degree of coordination burden present in the conventional response configuration.

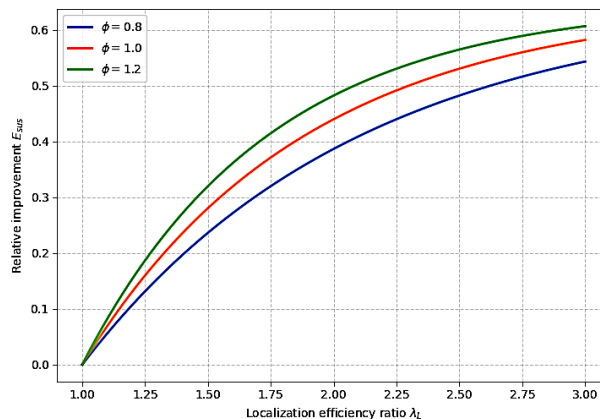


Figure 4. Relative response-time improvement as a function of deployment delay ratio under different levels of platform-orchestration effectiveness

8. Conclusions

This paper has presented a telematics-enabled digital coordination framework for mobile emergency decontamination in transport-hub environments. The framework was formulated as a cyber-physical safety-service model integrating operator interaction, application-layer control, equipment-level execution, and persistent audit-oriented data management. Its formal core combines deterministic lifecycle control, algebraic preset validation, access-governed operation, and latency-bounded command transfer.

The simulation-based validation confirmed the functional feasibility and technical consistency of the proposed approach. Across 18 structured scenarios, the prototype achieved a 100% pass rate, no critical or major defects, a data integrity index of 100%, and a non-functional compliance index of 95%. Command transmission remained within the admissible latency bound, with $L_{99} = 71$ ms against the required maximum of 200 ms. These results show that the framework is not only formally specified, but also implementable in a form suitable for time-sensitive emergency-response coordination.

The transport-hub case study further demonstrated the operational relevance of the proposed framework. In a hazardous-cargo port scenario, the integrated configuration reduced the mean time to operational readiness from 47.3 min to 27.4 min, corresponding to a 42% improvement relative to conventional manual coordination. From a transport-telematics perspective, this result indicates that digitally coordinated deployment of mobile safety services can contribute directly to local disruption containment and operational resilience in transport nodes.

The study therefore contributes in four principal ways: it formulates a transport-hub-oriented coordination model for mobile decontamination as a cyber-physical safety service; it integrates lifecycle control, preset consistency, and role-based operational access within a unified formal framework; it establishes a traceable scenario-based validation approach for this class of systems; and it quantifies the operational benefit of digital coordination in a realistic transport-hub emergency scenario.

At the same time, several limitations remain. The current validation was conducted in a simulated environment and should be extended through field testing with the physical mobile installation under live operational conditions. The response-time model used in the case study was parameterised by expert-based estimates and would benefit from calibration against empirical data from port emergency exercises. In addition, full GDPR-scope data protection remains to be implemented in the post-prototype phase. These limitations do not invalidate the present results, but define the main directions for future research and system maturation.

Taken together, the reported results show that mobile emergency decontamination can be interpreted not merely as an isolated technical intervention, but as a digitally coordinated transport-hub safety service. In this sense, the proposed framework provides both a formal reference model and an operationally relevant basis for further development of cyber-physical emergency-support systems in transport environments.

Appendix A. Complete functional and non-functional requirements

Table A1. Functional requirements (FR)

ID	Module	Description	Key constraint / formula	UC	NFR
FR-01	Presets	Create, edit, and delete Preset records	Record operations must be role-restricted (Admin, Operator)	UC-AL-3	07
FR-02	Presets	Store hot water volume V_h per Preset	$V_h > 0$	UC-AL-4	07
FR-03	Presets	Store cold water volume V_c per Preset	$V_c > 0$	UC-AL-4	07
FR-04	Presets	Store total volume V_i ; enforce balance	$V_h + V_c \leq V_i$ (reject if violated)	UC-AL-4	07, 13
FR-05	Presets	Persist Presets for reuse across processes	Preset available after session close	UC-AL-3, UC-AL-4	13, 14
FR-06	Presets	Transmit Preset to PLC on process start	$L_c^{omm} \leq L_{ma}^s = 200$ ms	UC-AL-4	09, 10
FR-07	Persons	Create and maintain person catalogue	Searchable; create & update operations	UC-AL-3	16
FR-08	Persons	Store mandatory person fields; enforce ID uniqueness	$ID(p_i) \neq ID(p_j)$ for all $i \neq j$	UC-AL-3	07, 08
FR-09	Persons	Edit person records with audit logging	All edits recorded in audit_log	UC-AL-3	08

ID	Module	Description	Key constraint / formula	UC	NFR
FR-10	Persons	Fast person retrieval by name or ID	Response ≤ 2 s for $N \leq 10,000$ records	UC-AL-3, UC-AL-4	15
FR-11	Decontam.	Create new decontamination process record	One Person + one Preset required	UC-AL-4	05
FR-12	Decontam.	Enforce Person + Preset pre-condition before RUN	RUN blocked without both associations	UC-AL-4	06, 07
FR-13	Decontam.	Execute RUN command; trigger $\delta(\text{READY}, \text{start}) = \text{RUNNING}$	Atomic state transition in M	UC-AL-4	05, 06
FR-14	Decontam.	Transmit Preset to PLC; log $t_{\text{sta}}^{R_i}$	PLC receives $\{V_b, V_c, V_i\}$; timestamp stored	UC-AL-4, UC-AL-5	09, 10
FR-15	Decontam.	Auto-record $\Delta t, V_a, \varepsilon$ on completion; lock read-only	is_readonly := TRUE on COMPLETED/ABORTED	UC-AL-7, UC-AL-8	13, 14

Table A2. Non-functional requirements (NFR)

ID	Category	Description	Threshold / metric	Verified in
NFR-01	Reliability	Stable operation under normal conditions	Availability $A \geq 0.995$	TC-CAT-1
NFR-02	Reliability	Data-loss-free sensor data processing	Zero sensor reading loss	TC-CAT-3
NFR-03	Reliability	State recovery after network disruption	Recovery within 60 s	TC-CAT-2
NFR-04	Reliability	Critical errors logged with timestamp	100% coverage in system_events	TC-CAT-5
NFR-05	Security	RBAC predicate on all API endpoints	HTTP 403 on $\Pi(u,o) = 0$	TC-CAT-5
NFR-06	Security	Process operations restricted to Admin/Operator	Guest cannot start/abort	TC-CAT-5
NFR-07	Security	Server-side input validation (GDPR-scope: partial)	Validation before storage/PLC	TC-CAT-1
NFR-08	Security	Immutable audit log for all state changes	100% of state ops logged	TC-CAT-5
NFR-09	PLC	Bidirectional channel with PLC	Modbus RTU 8N1 connection	TC-CAT-2
NFR-10	PLC	Command latency at 99th percentile	$L_{99} \leq 200$ ms	TC-CAT-2
NFR-11	PLC	Correct PLC signal interpretation	State transitions match PLC signals	TC-CAT-2
NFR-12	PLC	PLC fault notification within 5 s	Detected in $t^{\text{Dem}} = 1.1$ s	TC-CAT-2
NFR-13	Data	Schema-validated relational storage	DB constraint enforcement	TC-CAT-5
NFR-14	Data	Process records read-only on completion	is_readonly trigger verified	TC-CAT-5
NFR-15	Data	Historical query response ≤ 3 s	1,000-record result set	TC-CAT-1
NFR-16	Data	Referential integrity enforced at DB level	Delete of linked record rejected	TC-CAT-5
NFR-17	Usability	Primary workflows in ≤ 5 interactions	Full workflow ≤ 5 steps	TC-CAT-4
NFR-18	Usability	Key actions within ≤ 2 navigation steps	Start/abort reachable in 1–2 taps	TC-CAT-4
NFR-19	Usability	Unambiguous status notifications	Self-explanatory for 3/3 operators	TC-CAT-4
NFR-20	Usability	Consistent terminology throughout interface	No synonym conflicts observed	TC-CAT-4

Appendix B. Test scenario specifications (given-when-then)

Each scenario is classified by severity: Critical (C), Major (M), or Minor (O). All 18 scenarios are listed below.

TC-CAT-1: Functional System Testing

ID	Scenario	Severity	Given	When	Then
TC-PRS-01	Preset CRUD	C	Authenticated Operator; system online	Create Preset ($V_b=30L$, $V_c=70L$, $V_i=100L$); edit; delete	Preset saved; update reflected; record removed; active-Preset deletion blocked
TC-PRS-04	Balance validation	C	Preset editor open	Submit $V_b=60L$, $V_c=50L$, $V_i=100L$ (sum>total)	System rejects with validation error; no PLC transmission
TC-PER-01	Person creation	C	Authenticated Operator	Create Person with all mandatory fields	Record saved; searchable by name and ID
TC-PER-02	Mandatory fields	C	Person form open	Submit without Last Name and ID	Form rejected; missing-field messages displayed

ID	Scenario	Severity	Given	When	Then
TC-DEC-01	Process creation	C	Person and Preset exist; Operator authenticated	Create new process; select Person + Preset	Process record in state READY; RUN enabled
TC-DEC-03	Process RUN	C	Process in READY state	Press RUN	State $\rightarrow$ RUNNING; t_{sta}^R logged; Preset transmitted to PLC

TC-CAT-2: Hardware/PLC Integration Testing

ID	Scenario	Sev.	Given	When	Then
TC-PLC-01	Preset transmission	C	Process in RUNNING state; PLC online	System sends TransmitPreset command (N=200 repetitions)	PLC receives $\{V_h, V_c, V_i\}$; $L_{90V}=47ms$, $L_{99}=71ms \ll 200ms$
TC-PLC-02	PLC fault detection	C	Active decontamination process	Simulate PLC communication interruption $\tau=3s$	Fault detected in $t^{Dem}=1.1s$; operator notified; new process blocked
TC-HW-01	Signal integrity	C	Control board powered; all actuators connected	Issue open/close commands to all valve channels	All actuators respond; no cross-channel interference
TC-HW-02	Overcurrent protection	C	Actuator channel loaded to $I_{ma}^x=2A$	Apply step overload to channel	Polyfuse trips; channel isolated; other channels unaffected

TC-CAT-3: Multi-Scenario Operational Testing

ID	Scenario	Sev.	Given	When	Then
TC-OPS-01	Normal sustained load	C	System operational; 1 operator session	Run continuous process for 30 min ($T_s=500ms$, $N_s=3600$ readings)	Zero data loss; no state anomalies; report generated
TC-OPS-02	Elevated load (3 sessions)	C	Three concurrent Operator sessions	Each session creates and runs an independent process	State vectors independent; no cross-session data leakage
TC-OPS-03	Sensor anomaly injection	C	Active process; sensors nominal	Inject: (a) step change $\varepsilon>5\%$; (b) dropout $\tau=2s$; (c) out-of-range value	Alert generated for each; no uncontrolled state transition
TC-OPS-04	Emergency abort	C	Process in RUNNING state	Operator presses Emergency Abort	State $\rightarrow$ EMERGENCY in $t_s=340ms$; further initiation blocked until reset

TC-CAT-4: UI/UX Usability Testing

ID	Scenario	Sev.	Given	When	Then
TC-UX-01	Full workflow completion	M	3 operators; no prior software training	Complete: login $\rightarrow$ Preset create $\rightarrow$ Person create $\rightarrow$ RUN $\rightarrow$ report	All 3 complete without abandonment; $\bar{t}=3.2min$
TC-UX-02	Navigation depth	M	Authenticated session	Access Start, Emergency Abort, Equipment Selection from home	All reachable in ≤ 2 steps (NFR-18 satisfied)
TC-UX-03	Error message comprehension	M	Operator attempts invalid Preset submission	Submit form with $V_h+V_c>V_i$; empty mandatory field	All 3 operators interpret messages correctly without clarification
TC-UX-04	Minor ergonomic observations	O	Post-task feedback session	Collect verbal feedback on interface elements	3 Minor observations: button placement; status hierarchy; timer font

TC-CAT-5: Data Registration and Access Control Testing

ID	Scenario	Sev.	Given	When	Then
TC-DEC-05	Process record completeness	C	Process in COMPLETED state	Inspect decontamination_processes record	All 12 columns populated; is_readonly=TRUE; Δt , V_a , ε recorded
TC-REP-01	Report generation	C	Completed process exists	Generate report via UC-AL-8.0	Structured report produced; data read-only confirmed
TC-SEC-01	RBAC enforcement	C	Operator session authenticated	Attempt: system config, user management, Preset delete (restricted operations)	HTTP 403 returned; 3 audit_log entries created; no state change
TC-SEC-02	Referential integrity	C	Person record linked to completed process	Attempt deletion of Person record	DB rejects with FK constraint error; record preserved (NFR-16)

Acknowledgements

The research leading to these results has received funding from the project “Competence Centre of Information and Communication Technologies for Research” of the Recovery and Resilience Facility, contract No. 5.1.1.2.i.0/2/24/A/CFLA/007 signed between IT Competence Centre and Central Finance and Contracts Agency, Research No. 1.8 “Arete Logic: Intelligent control system for decontamination equipment”.

Declaration of Generative AI and AI-assisted technologies in the writing process:

During the preparation of this manuscript, the authors used ChatGPT to improve the English language and readability of the text. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

1. Ahmed, S. and Dey, K. (2020) Resilience modelling concepts in transportation systems: A comprehensive review based on mode, and modelling techniques. *Journal of Infrastructure Preservation and Resilience*, 1, 1. DOI:10.1186/s43065-020-00008-9.
2. Arete. (2026) *Superstructures and platforms*. Available at: <https://www.aretetech.com/superstructures-and-platforms/>, last accessed 01 Apr 2026.
3. Aslam, M.M., Shafik, W., Hidayatullah, A.F., Kalinaki, K., Gul, H., Zakari, R.Y. and Tufail, A. (2025) Intelligent transportation systems: A critical review of integration of cyber-physical systems (CPS) and industry 4.0. *Digital Communications and Networks*, 12(1), 143-164. DOI:10.1016/j.dcan.2025.06.014.
4. Avci, İ. and Koca, M. (2024) Intelligent transportation system technologies, challenges and security. *Applied Sciences*, 14(11), 4646. DOI:10.3390/app14114646.
5. Carter, H., Drury, J., Rubin, G.J., Williams, R. and Amlôt, R. (2012) Public experiences of mass casualty decontamination. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 10(3), 280–289. DOI:10.1089/bsp.2012.0013.
6. Carter, H., Drury, J., Rubin, G.J., Williams, R.J. and Amlôt, R. (2014) Effective responder communication improves efficiency and psychological outcomes in a mass decontamination field. *PLOS ONE*, 9(3), e89846. DOI:10.1371/journal.pone.0089846.
7. Carter, H. and Amlôt, R. (2016) Mass casualty decontamination guidance and psychosocial aspects of CBRN incident management: A review and synthesis. *PLOS Currents Disasters*, 8. DOI:10.1371/currents.dis.c2d3d652d9d07a2a620ed5429e017ef5.
8. Cassandras, C.G. and Lafortune, S. (2008) *Introduction to Discrete Event Systems*. 2nd edn. New York: Springer.
9. Chilcott, R.P. (2014) Managing mass casualties and decontamination. *Environment International*, 72, 37–45. DOI:10.1016/j.envint.2014.02.006.
10. Cibulsky, S.M., Sokolowski, D., Lafontaine, M., Gagnon, C., Blain, P.G., Russell, D., Kreppel, H., Biederbick, W., Shimazu, T., Kondo, H., Saito, T., Jourdain, J.R., Paquet, F., Li, C., Akashi, M., Tatsuzaki, H., Prosser, L. (2015) Mass casualty decontamination in a chemical or radiological/nuclear incident with external contamination: Guiding principles and research needs. *PLOS Currents Disasters*, 7. DOI: 10.1371/currents.dis.9489f4c319d9105dd0f1435ca182eaa9.
11. Collins, S., James, T., Carter, H., Symons, C., Southworth, F., Foxall, K., Marczylo, T. and Amlot, R. (2021) Mass casualty decontamination for chemical incidents: research outcomes and future priorities. *International Journal of Environmental Research and Public Health*, 18(6), 3079. DOI:10.3390/ijerph18063079.
12. Currie, J. and Heslop, D.J. (2018) Operational systems evaluation of a large-scale multi-agency decontamination exercise. *International Journal of Disaster Risk Reduction*, 31, 821–830. DOI:10.1016/j.ijdrr.2018.03.027.
13. Dennis, A., Weston, D., Amlôt, R., Arnold, A., Carbon, D., Carter, H. (2023) The role of pre-incident information and responder communication in effective management of casualties, including members of vulnerable groups, during a decontamination field exercise. *International Journal of Disaster Risk Reduction*, 94, 103806. DOI:10.1016/j.ijdrr.2023.103806.
14. Ferraiolo, D., Sandhu, R., Gavrilu, S., Kuhn, D.R. and Chandramouli, R. (2001) Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3), 224–274. DOI:10.1145/501978.501980.

15. Holloway, C.M. and Butler, R.W. (1996) *Fault tree analysis of a digital flight control system*. NASA Technical Memorandum 110180. Hampton: NASA Langley Research Center.
16. Lee, D.-H., Kim, C.-M., Song, H.-S., Lee, Y.-H. and Chung, W.-S. (2023) Simulation-based cybersecurity testing and evaluation method for connected car V2X application using virtual machine. *Sensors*, 23(3), 1421. DOI:10.3390/s23031421.
17. Levitin, H.W., Siegelson, H.J., Dickinson, S., Halpern, P., Haraguchi, Y., Nocera, A., Turineck, D. (2003) Decontamination of mass casualties — Re-evaluating existing dogma. *Prehospital and Disaster Medicine*, 18(3), 200–207. DOI:10.1017/S1049023X00001060.
18. O’Kelly, M.E. (2025) Transportation security at hubs: Addressing key challenges across modes of transport. *Journal of Transportation Security*, 18, 4. DOI:10.1007/s12198-025-00294-y.
19. Pavão, J., Bastardo, R. and Rocha, N.P. (2024) Cyber resilience and intelligent transport systems, a scoping review. *Procedia Computer Science*, 239, 139–148. DOI:10.1016/j.procs.2024.06.156.
20. Riedmaier, S., Schneider, D., Watzenig, D., Diermeyer, F., Schick, B. (2021) Model validation and scenario selection for virtual-based homologation of automated vehicles. *Applied Sciences*, 11(1), 35. DOI:10.3390/app11010035.
21. Sandhu, R.S., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (1996) Role-based access control models. *IEEE Computer*, 29(2), 38–47. DOI:10.1109/2.485845.
22. Stouffer, K., Falco, J. and Scarfone, K. (2011) *Guide to industrial control systems (ICS) security*. NIST Special Publication 800-82. Gaithersburg: National Institute of Standards and Technology.
23. Vyatkin, V. (2013) Software engineering in industrial automation: State-of-the-art review. *IEEE Transactions on Industrial Informatics*, 9(3), 1234–1249. DOI:10.1109/TII.2013.2258165.
24. Wiśniewski, R., Bazyło, G., Szcześniak, P., Grobelna, I. and Wojnakowski, M. (2019) Design and verification of cyber-physical systems specified by Petri nets: A case study of a direct matrix converter. *Mathematics*, 7(9), 812. DOI:10.3390/math7090812.
25. Zhang, X., Lu, Y., Wang, J., Yuan, D. and Huang, X. (2023) Quantifying road transport resilience to emergencies: Evidence from China. *Sustainability*, 15(20), 14956. DOI:10.3390/su152014956.