Review

Not peer-reviewed version

Bridging the Information Gap in Emergency Response: A Hybrid Model for Digital Fire Safety Instructions

Patryk Krupa * and Péter Pántya

Posted Date: 26 February 2026

doi: 10.20944/preprints202602.1571.v1

Keywords: fire safety instructions; hybrid documentation; pre-incident planning; minimum operational dataset; progressive web apps; QR codes; offline-first; quishing

Review

Bridging the Information Gap in Emergency Response: A Hybrid Model for Digital Fire Safety Instructions

Patryk Krupa [1,*] and Péter Pántya [2]

[1] University of Zielona Góra, Faculty of Engineering and Technical Sciences, Institute of Materials Engineering and Biomedical Engineering, Prof. Z. Szafrana Street 4, 65-516 Zielona Góra, Poland

[2] Ludovika University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, Department of Fire Protection and Rescue Control, Ludovika tér 2, H-1083 Budapest, Hungary

* Correspondence: pkrupa@uz.zgora.pl

Featured application

Implementation of a hybrid documentation model (paper master + digital overlay) using offline-first Progressive Web Apps (PWA) and QR codes to minimize time-to-information for emergency responders in complex building infrastructures.

Abstract

Rapid access to building intelligence is critical for emergency response, yet paper Fire Safety Instructions (FSi) often provide limited utility under stress. This structured narrative review addresses the "information gap" between unit arrival and decision-making by analyzing legal admissibility, technological requirements, and security risks of digital FSi across Poland, Germany, France, Belgium, and Hungary. While no explicit prohibition of digital forms was identified, enforcement practices prioritize paper as the evidentiary master. Consequently, we propose a hybrid model: a paper master for compliance and redundancy, supplemented by a digital operational overlay accessed via "zero-install" offline-first Progressive Web Apps (PWA). The review defines a Minimum Operational Dataset (MOD)—prioritizing critical data like utility shut-offs and hazards over full documentation—and addresses cybersecurity threats, specifically QR-phishing ("quishing"). We conclude that the hybrid model minimizes legal and operational risks while significantly reducing time-to-information, provided that strict content identity and change management protocols are maintained.

Keywords: fire safety instructions; hybrid documentation; pre-incident planning; minimum operational dataset; progressive web apps; QR codes; offline-first; quishing

1. Introduction

Modern fire safety engineering increasingly integrates advanced detection, intelligent monitoring, and IoT-enabled building systems. Despite this progress, on-scene access to building intelligence still relies largely on analog artifacts. Paper fire safety instructions (FSi/IBP), typically stored inside the building (often in a dedicated metal cabinet), may be difficult to locate and use under smoke, stress, and time pressure. Yet the initial phase of an incident requires rapid decisions on reconnaissance, allocation of resources, and firefighter safety. Delays in obtaining key information—such as utility shut-offs, explosive atmospheres, hydrant locations, or critical control panels—increase the likelihood of errors.

This creates an operational "information gap": the time between first unit arrival and the acquisition of decision-critical building information. Digital delivery via QR codes and browser-

 doi:10.20944/preprints202602.1571.v1

based solutions (including progressive web apps, PWA) could reduce this gap by enabling fast access from standard mobile devices. However, implementation faces three categories of barriers:

- Legal: do regulations and enforcement practice allow replacing or at least supplementing paper documents with a digital operational layer?
- Technological: how to ensure reliable access during outages (power, connectivity) and under degraded conditions?
- Security: how to mitigate misuse and deception (e.g., quishing), and how to preserve integrity and trust?

This article provides a structured narrative review combining legal analysis (Poland and selected EU countries) with requirements from fire safety engineering, human factors, and cybersecurity. The central thesis is that—under current regulatory and reliability constraints—a hybrid model is preferable, where the digital layer supports but does not replace the paper master document..

2. Materials and Methods

A structured narrative review approach was adopted to synthesize heterogeneous evidence across law/regulation, information systems, and operational firefighting practice. The selection and reporting logic follows narrative review quality criteria and transparent reporting principles [1–3].

2.1. Search Strategy and Selection

The primary literature search covered 2015–2026 in Scopus, Web of Science, and Google Scholar. The lower bound (2015) was chosen to reflect the maturation of smartphone ecosystems and offline-capable web technologies that enable meaningful analysis of "zero-install" architectures (e.g., Service Workers/PWA) [23]. A detailed search log (databases, search strings in English and Polish, dates of search execution, record counts, and screening decisions) are reported in Supplementary Table S1 to ensure full transparency and reproducibility. Targeted backward searches (snowballing) were additionally used to include seminal earlier work on decision-making, situation awareness, and key responder information needs, as well as early evidence on QR/PWA security where needed. Earlier sources were retained when foundational for constructs used in this review (e.g., situational awareness, naturalistic decision making) or when repeatedly cited in responder information needs and pre-incident planning literature. English and Polish keyword combinations included: fire safety plan digitalization, electronic fire safety instructions, pre-incident planning, QR codes in emergency response, mobile technology in fire service, cognitive load, situational awareness, naturalistic decision making, and service worker security.

In parallel, we analyzed laws, standards, and institutional guidance relevant to building fire safety documentation and emergency response for Poland (PL), Germany (DE), France (FR), Belgium (BE), and Hungary (HU). Country selection was justified by diversity in administrative models and operational practices.

2.2. Inclusion and Exclusion Criteria

Included sources comprised: peer-reviewed publications, legal acts, technical standards, and institutional/industry guidance (grey literature) to enable triangulation across legal, technological, and operational perspectives.

Excluded were: (i) training/simulation-oriented solutions, because the focus is operational information distribution during real incidents; (ii) solutions designed exclusively for wearables (e.g., smartwatch-only interfaces); and (iii) publications prior to 2010, except **seminal** work that is foundational for the constructs used in this review (e.g., situation awareness, naturalistic decision-making) or repeatedly cited in responder information needs and pre-incident planning research. The 2015–2026 window (with limited pre-2010 exceptions) was adopted to reflect the stabilization of the smartphone paradigm and the maturation of offline-capable web technologies enabling "offline-first/zero-install" architectures (notably Service Workers/PWA after ~2015).

 doi:10.20944/preprints202602.1571.v1

2.3. Methodological Limitations

This review is conceptual and integrative; it does not evaluate a single commercial system. Operational validation—particularly identification of "critical information" most often used by firefighters—should be addressed in future empirical studies (case studies, usability testing, Delphi methods).

3. Results: Legal and Regulatory Context

Digital implementation must account for a common regulatory pattern: many requirements specify the obligation to have and make available safety information, but rarely prescribe a single medium (paper vs. electronic). The key question is whether the digital layer can be legally equivalent or should remain an operational copy/overlay.

3.1. Poland: Interpretive Legal Assessment

In Poland, the core obligation to develop fire safety instructions (IBP) is set by the Regulation of the Minister of the Interior and Administration of 7 June 2010 [4]. Two issues are central for digitalization: (i) the requirement that instructions are accessible to rescue teams, and (ii) the relationship between IBP and pre-incident/operational planning by the State Fire Service (PSP) and other responders [5,6].

A linguistic and purposive interpretation yields three practical conclusions:

- No explicit medium is defined: the regulation emphasizes possession and accessibility, not a mandatory paper-only form.
- Enforcement practice strengthens paper's evidentiary role: in routine compliance audits and documentation workflows, a physical document with clear authenticity cues (signatures, revision dates) remains the default evidentiary artifact; therefore, paper functions as the master document for accountability and archiving, while the digital layer is best treated as a controlled operational copy/overlay.
- Hybrid model as conservative compliance: since copying is not prohibited, a digital operational overlay (e.g., via QR codes at controlled access points) is not expressly prohibited, provided it does not eliminate the paper master expected in practice.

A broader EU evidentiary context is provided by the eIDAS framework for electronic identification and trust services; however, compliance and inspection workflows in building fire safety still rely heavily on practical authenticity cues and predictable availability, which supports retaining paper as the master while treating the digital layer as a controlled operational overlay [7].

Operationally, the digital layer should be treated as an operational overlay designed to reduce the information gap during the first minutes, while paper remains the legal/evidentiary master and an analog fallback for outages.

3.2. European Comparative Perspective

Across the selected EU countries, a similar pattern is observed: physical availability of intervention documentation at the object level is preserved, while digital solutions increasingly support distribution and updates.

Table 1. Legal status of digital fire safety instructions (or equivalents) in selected EU countries. Source: authors' synthesis based on analyzed acts/standards [4,8–11].

To reduce ambiguity, Table 1 should be read as a functional comparison of availability, traceability, and accountability requirements rather than a claim of administrative equivalence of document types; key reference anchors per jurisdiction include PL [4], DE [8,12], FR [9,13], BE [10,14], and HU [11].

Table 1. Legal status of digital fire safety instructions (or equivalents) in selected EU countries.

 doi:10.20944/preprints202602.1571.v1

Country	Document (equivalent)	Medium requirement in practice	Status of electronic version	Primary legal/operational risk
PL	Fire safety instructions (IBP)	Not defined explicitly; typically paper	Acceptable as copy/operational overlay	Content divergence between paper and digital
DE	Fire brigade plans (Feuerwehrpläne)	Strongly standardized; paper on site, CAD upstream	Common supplemental channel	Symbol/format compliance with DIN 14095
FR	Intervention plan (ERP/other regimes)	Physical plan at defined locations	Central systems (e.g., ETARE) as complement	Dependence on power/connectivity
BE	Intervention file (dossier d'intervention)	Zone-dependent	Increasingly promoted/integrated	Lack of uniform national access standard
HU	Fire protection documentation (OTSZ regime)	Paper preferred for inspections	Mostly voluntary/unclear	Non-recognition during preventive inspections

Terminological mapping and functional equivalence. The "equivalents" summarized in Table 1 are not interchangeable documents in an administrative sense; they differ in authorship, mandatory content, and the point in the response cycle where they are used. In Germany, Feuerwehrpläne are tightly standardized (DIN 14095) and are increasingly complemented by digitization efforts that emphasize interoperability and georeferencing for operational use [8,12]. In France, ETARE plans represent an intervention planning instrument within the fire service prevision framework and are typically maintained/used by SDIS for "établissements répertoriés" [13]. In Belgium, the dossier d'intervention is linked to workplace fire prevention obligations and has a prescribed minimum content (including a plan, intervention procedures, and key system information) [10,14]. This heterogeneity motivates interpreting "legal admissibility" in functional terms (availability, traceability, accountability) rather than as direct document equivalence across jurisdictions.

3.3. Synthesis: Principle of Dual Availability

The comparative results support a dual availability principle:

1. Material availability (paper fallback): a paper master document stored at a predictable, secure location (e.g., metal cabinet or deposit box) ensures access under infrastructure degradation (blackout, network failure, mechanical damage).
2. Operational availability (digital overlay): e-FSi provides rapid access to a minimal operational subset in the initial phase, e.g., via QR codes.

Therefore, fully paperless approaches currently carry elevated legal and reliability risk. The hybrid model is conservative and operationally advantageous, provided that content identity (paper vs. digital) and robust change management (versioning, traceability, audit) are implemented.

4. Results: Technological and Human Factors Framework

The "technology of e-FSi" is not an end in itself; it is a delivery mechanism for decision-relevant information under stress. Design should shift from "show the document" to meeting non-functional requirements: availability at the moment of need, low time-to-information, and resilience under degraded conditions.

4.1. Availability and Reliability Requirements

Pre-incident planning literature emphasizes that poor accessibility of plans reduces actionable information for first arriving commanders and increases reliance on external observation [15]. Standards such as NFPA 1620 highlight the need for standardized content and periodic verification,

 doi:10.20944/preprints202602.1571.v1

reinforcing the role of versioning and update control in e-FSi [5]. Incident management guidance further stresses coherent information flow and traceable responsibility [16].

Consequently, e-FSi should provide at minimum: (i) a deterministic access path (predictable entry point), (ii) offline capability or controlled functional degradation, (iii) separation of critical data (Level 0) from reference content (Levels 1–2), and (iv) versioning and traceability aligned with the paper master.

4.2. Distribution Channels: QR as an Entry Point

QR codes are standardized in ISO/IEC 18004 [17]. In the hybrid model, QR should function as an entry pointer to the operational overlay rather than a carrier of the operational content itself. Reliability depends strongly on physical placement.

A multi-point distribution strategy is recommended:

- Early access point (design recommendation): gate/entrance/guardhouse—where reconnaissance often begins before entering the building; in practice, the tag should be placed on the inside of the gate/perimeter fence (out of sight to passers-by) but reachable from the public side without delaying entry, following predictable placement conventions used for safety information and evacuation signage (e.g., ISO 23601) [18], while employing weather-resistant materials and anti-tamper mounting to risks.
- Confirmation/documentation point: near the paper master (cabinet/deposit box) to explicitly bind digital content to the master document and its revision control.

This aligns with predictable placement principles used for safety plans and signage (e.g., ISO 23601) [18]. This placement strategy should be treated as a design recommendation derived from minimizing time-to-information and limiting exposure to tampering, and should be empirically validated in future work (e.g., drills or usability tests under time pressure).

4.3. Access Architectures: PDF vs. Native App vs. PWA

Three approaches dominate: (1) static files (typically PDF), (2) native apps, and (3) web apps in a PWA architecture.

- Static PDF is simple to distribute but weak in change management: parallel versions proliferate, and usability under stress is limited.
- Native apps can offer robust offline operation but introduce high friction due to installation requirements, dependence on app stores, and Mobile Device Management (MDM) overhead—contrary to the "zero-install" operational needs of diverse response units [20–22].
- PWA offers a practical compromise: browser-based access with offline capability via Service Worker and caching APIs [23–26]. This enables an offline-first design where the minimal critical dataset is available even without network connectivity, provided that caching, update policies, and version governance are explicitly engineered and tested. In this review, the PWA argument is treated as a trade-off analysis: PWAs reduce installation friction ("zero-install") but introduce specific operational and security requirements (Service Worker scope control, cache integrity, rollback strategy) that must be managed.

Table 2. Comparison of distribution approaches for operational use.

Criterion	Paper (master)	PDF (static)	Native app	PWA (offline-first)
"Zero-install"	n/a	High (if locally stored)	Low	High
Offline operation	High	Variable	High	High (Service Worker + cache)
Update control	Manual	High divergence risk	Controlled, but store/MDM dependent	Controlled (versioning + cache strategy)
Usability under stress	Low–medium	Low–medium	Variable	High if UI is optimized

 doi:10.20944/preprints202602.1571.v1

Resilience to connectivity loss	High	Variable	High	High
Change auditability	Medium (signatures/dates)	Low–medium	Medium–high	Potentially high (logs, versions)
Key technical risks	Low	Medium	Medium–high	Medium

Source: authors' synthesis based on [19–26,29–32].

4.4. Human Factors: Designing for Incident Commanders and Firefighters

Operational conditions (time pressure, cognitive load, gloves, variable visibility) require human-centred design [27,28]. Situational awareness theory highlights the perception–comprehension–projection cycle [33], while naturalistic decision-making research shows that experienced commanders often act by rapid pattern recognition; therefore, "time-to-first useful information" is a critical metric [34]. Cognitive load theory warns against interface-driven overload [35]. Complementary UI principles—such as overview-to-detail navigation and information-foraging behavior—support designing interfaces that help commanders quickly locate the next "most valuable" item under pressure [36–38].

Therefore, e-FSi should implement progressive disclosure: Level 0 first (critical, short, highly legible), then Level 1 (tactical), then Level 2 (reference) on demand. Large touch targets are necessary given glove-related dexterity reduction [28]. WCAG 2.2 introduces a minimum target size requirement (24 × 24 CSS px) and an enhanced target size (44 × 44 CSS px) [29,30]; mobile platform guidance commonly recommends larger targets (e.g., 48 × 48 dp in Android/Material) [31,32]. WCAG also requires sufficient contrast and readability [29].

5. Results: Minimum Operational Dataset (MOD)

A digital layer is not useful as a screen-faithful copy of a full paper manual. In the first minutes, information value depends on prioritization, minimal cognitive cost, and deterministic availability—not completeness [33–35,39–41,45]. Hence, we propose a Minimum operational dataset (MOD) as a structuring framework for the operational overlay. Importantly, MOD is presented as a literature-informed framework distilled from recurring responder information needs and human-factors evidence, not as an empirically validated standard; its concrete field set and thresholds require operational validation (e.g., Delphi panels and field usability tests).

5.1. Definition and Role in the Hybrid Model

In a hybrid model, MOD bridges formal building documentation and responders' information needs. It aims to reduce the information gap by delivering the first useful information without searching a multi-page document. The concept aligns with pre-incident planning practices stressing standardized content and periodic verification [5,46].

For credibility, MOD should be (i) explicitly tied to the paper master revision (a shared version identifier), and (ii) maintained via traceable change management to reduce divergence.

5.2. Layered Structure: MOD Levels 0–2

A practical compromise is a three-level structure:

- MOD Level 0 (critical; early phase): utility shut-offs, high-risk zones, external hydrants/water sources, essential access/orientation cues—deterministically available offline.
- MOD Level 1 (tactical; subsequent phase): simplified floor/fire compartment plans, fire safety systems overview and control logic, technical rooms, key access information, contacts.
- MOD Level 2 (reference; extended operations): detailed schematics, SDS/chemical details, deeper technical documentation—possibly document-style but indexed.

Table 3. Proposed MOD structure (Levels 0–2) and preferred presentation formats.

 doi:10.20944/preprints202602.1571.v1

Information domain	Level 0 (critical)	Level 1 (tactical)	Level 2 (reference)	Preferred format
Access & ID	address, entrances, early QR point	access map, deposit points	detailed documents	card + map
Water	hydrants/sources	FDC/pumps/valves	calculations/parameters	map + schematic
Utilities	main shut-offs	switch rooms/technical spaces	installation schematics	list + schematic
Special hazards	key hazard zones	quantities/locations	SDS/procedures	icons + links (using standardized emergency symbols where feasible) [47]
Building layout	simple orientation sketch	simplified floor/zone plans	technical drawings	layered map
Fire safety systems	control panels locations	control dependencies	full documentation	card + diagram
Contacts	24/7 functional number	roles list	responsibilities	card
Constraints	stable “no-go” hazards	access restrictions	structural/engineering data	card + links

Source: authors’ synthesis based on [5,33–35,39–45].

5.3. Proposed MOD Content Categories

Building on NIST guidance on responder information needs [39–41] and studies on information processing and task-analysis–derived requirement models for fireground decision support [45,46], MOD content can be organized into eight cross-building categories:

A. Identification and access; B. Water supply; C. Utility shut-offs; D. Special hazards and dangerous substances; E. Internal orientation; F. Fire safety systems; G. People and responsibility (contacts); H. Operational constraints.

This structure is intentionally stable across building types, enabling predictable navigation and lower cognitive cost during incidents.

6. Results: Security, Privacy, and Risk Management

The operational overlay delivered via QR/PWA is part of a socio-technical system. Failure, manipulation, or disinformation can directly translate into decision errors. Two key conclusions emerge: (i) dominant risks are socio-technical (physical manipulation + social engineering + web/application weaknesses), and (ii) a hybrid model reduces single-point-of-failure sensitivity if content identity and change control are enforced.

6.1. Security Objectives and Protected Assets

Using the CIA triad, Level 0 prioritizes integrity and availability: wrong utility shut-off or hazard location information is more dangerous than disclosure. For Levels 1–2, confidentiality becomes more relevant (detailed plans and security-sensitive data). Protected assets include: (i) content identity between paper and digital, (ii) access channel (QR/URL, DNS, TLS), (iii) caching/update mechanisms (Service Worker), and (iv) endpoint devices storing offline content.

6.2. Quishing and Physical Manipulation of QR Codes

QR-phishing (“quishing”) is a low-cost attack where a malicious code is overlaid onto a legitimate one, redirecting users to a fraudulent resource. Empirical and survey research shows limited user ability to verify encoded content and a strong tendency to “auto-trust” QR codes in high-trust environments [50–53]. Therefore, QR should not be the sole trust mechanism.

Practical mitigations (physical + operational):

 doi:10.20944/preprints202602.1571.v1

- Tamper resistance: metal plates, anti-tamper fasteners, tamper-evident labels ("VOID"), placement within CCTV coverage, and scheduled physical inspections.
- Reducing QR "power": encode a building identifier rather than a full URL; force access through a fixed, known domain (allow-listing).
- User-visible verification: show the destination domain and building ID before loading detailed content; warn on redirects outside trusted domains.
- Controlled redundancy: multiple QR points improve availability but increase attack surface; mitigate by content segmentation (gate: Level 0; cabinet: Level 1–2) and inspection procedures.

Government and sector advisories reinforce that QR codes are now a mainstream social-engineering vector, not only an academic concern. Guidance from CISA and the U.S. HHS HC3 highlights QR-code phishing as a practical attack path, while IC3 reports document state-sponsored campaigns leveraging malicious QR codes for initial access [52–54]. For safety-critical deployments, this supports treating the QR token as a high-risk entry channel that requires both physical hardening and digital verification.

Hardening the QR token: authenticated identifiers. Beyond tamper-evident mounting, the hybrid model can increase trust by separating (i) an untrusted physical pointer (QR) from (ii) a verifiable digital identity. A practical pattern is to encode only a short building identifier plus an authenticity tag (e.g., a digital signature or MAC) that the PWA verifies offline using a pinned public key or shared secret, rejecting modified identifiers. ISO/IEC 20248 provides data structures for authenticity/traceability metadata in 2D symbols, and cryptographic QR-code schemes have been proposed specifically to reduce phishing and tampering risks [55–57]. Operationally, pairing this with a human-readable building code printed next to the symbol (for verbal cross-check with dispatch/owners) adds a low-cost, low-tech verification channel.

6.3. PWA Risks: Service Worker Persistence and Cache Integrity

Offline-first PWA relies on Service Workers and Cache Storage; these mechanisms can also preserve compromised states if misdesigned. Research indicates long persistence windows and specific threat classes such as Service Worker-assisted XSS, privacy misuse, and cache poisoning [58–61].

Design implications:

1. Minimize attack surface: avoid third-party scripts; minimize dependencies; constrain Service Worker scope.
2. Enforce integrity: strong CSP, Subresource Integrity (SRI) for static assets, strict HTTPS/HSTS.
3. Manage staleness: explicit revision numbers aligned with the paper master, TTL policies, and clear "last updated" indicators.
4. Rollback/kill switch: capability to quickly withdraw a faulty version while preserving minimal critical access.

6.4. Privacy and Sensitive Information Exposure

Risks involve both personal data (contacts) and security-sensitive information (detailed plans, control logic). GDPR principles (minimization, privacy by design) apply [62]. NIS2 strengthens expectations for risk management and resilience in relevant entities [63], while ENISA threat landscapes repeatedly highlight social engineering as a dominant vector [64].

Practical balancing measures include minimizing personal data in Level 0 (functional duty phone), segmenting content by risk (Level 0 public-facing; Level 1–2 behind an **infrastructure-independent** on-site second factor (**e.g., a static access code printed and stored inside the physical master cabinet**, or a physical key token), ensuring access even in zero-connectivity zones like basements), and logging changes to ensure accountability. In addition to version identifiers, maintaining protected change logs (who changed what, when) and operational access logs—

 doi:10.20944/preprints202602.1571.v1

implemented with minimization and retention rules—helps defend against disputes and supports post-incident learning; NIST guidance on log management provides a baseline for integrity, retention, and monitoring controls [66].

Table 4. Key e-FSi risks and example mitigations.

Risk area	Mechanism	Operational impact	Example mitigations
Quishing / QR replacement	sticker overlay, malicious redirect	disinformation, delay, data theft	tamper-evident labels, inspections, allow-listed domain, QR as ID (not URL), Level 0 vs 1–2 separation
Content spoofing	fake domain/DNS/rehosting	wrong decisions, loss of trust	fixed domain, HTTPS/HSTS, verifiable versions, redirect restrictions
PWA/Service Worker abuse	persistence, SW-XSS	offline disinformation	CSP/SRI, minimized dependencies, constrained scope, controlled update/rollback
Cache availability/staleness	cache poisoning, poor caching strategy	outage or outdated data	versioned cache, TTL, explicit revision display, controlled degradation
Confidentiality exposure	excessive Level 1–2 access	physical security risk, compliance issues	content segmentation, on-site second factor, minimization, audit

Source: authors' synthesis based on [50–66].

7. Discussion

7.1. Positioning Within Pre-Incident Planning and Building Intelligence Research

The core question is not whether to digitize, but what operational function the digital layer should serve in a high-risk domain. The proposed e-FSi as an operational overlay aligns with pre-incident planning emphasis on availability, currency, and standardization rather than document replication in the field [16,46]. NIST work on "building intelligence" similarly stresses that effectiveness depends on aligning data with decisions under time pressure [40,41]. MOD operationalizes this concept as a simple layered structure designed for zero-install access.

7.2. Limits of Fully Paperless Models and the Rationale for Redundancy

A paperless approach increases boundary conditions for availability and trust (power, connectivity, device function, cache integrity, QR manipulation). In dynamic high-risk operations, safety is achieved through layered defenses and redundancy (e.g., the "Swiss cheese" model) [67,68]. In this context, "paper as master + digital as operational overlay" is not a mere organizational compromise but a resilience mechanism.

7.3. MOD as an Interoperability and Coordination Mechanism

MOD's value lies not only in content fields but also in acting as a shared information standard between building owners, maintenance teams, prevention services, and responders. Research on coordination during multi-agency response suggests persistent challenges in information sharing, standardization, and common understanding [69–71]. A stable MOD template can lower friction: it is easier to maintain, audit, and teach than a full manual, and it makes responders' expectations more predictable. This is consistent with evidence that firefighter acceptance of response information systems depends on perceived usefulness and fit to operational workflows [71].

7.4. Effectiveness Metrics and Evaluation Design

Evaluation should move beyond compliance and IT security to measurable operational indicators: time to Level 0 from arrival, navigation error rates, paper-digital revision consistency in audits, and offline performance under degraded connectivity. These metrics support empirically grounded decisions on minimal viable trust and maintenance mechanisms.

 doi:10.20944/preprints202602.1571.v1

7.5. Limitations and Future Research

This review integrates heterogeneous sources, limiting claims of full legal equivalence across jurisdictions because enforcement practice varies locally. Some arguments transfer general human-factors and cybersecurity findings to e-FSi; context-specific validation is required.

Future work should include: (i) case studies across building risk profiles; (ii) usability tests with firefighters under realistic constraints (gloves, smoke, time pressure); (iii) Delphi/expert elicitation to identify the most critical Level 0 fields; and (iv) stress-testing for degradation scenarios (loss of connectivity, QR manipulation, version divergence).

8. Conclusions

Across Poland and the selected EU countries, no explicit prohibition of digital representations of fire safety instructions was identified; nevertheless, enforcement practice and evidentiary needs preserve the paper document as the master reference. This distinction is not merely administrative: it reflects how authenticity is demonstrated (signatures, revision dates, controlled storage) and how responsibility for content is assigned during audits and post-incident review. Under current reliability constraints (power and connectivity loss, device failure, and physical manipulation of access tokens such as QR labels), fully paperless models remain higher-risk because they concentrate availability and trust in a single technological chain. A hybrid approach—paper master plus a carefully designed digital operational overlay—therefore offers a resilient and operationally beneficial pathway, combining legal defensibility with faster time-to-information.

However, the hybrid model is only as credible as its change control. If the operational overlay is allowed to drift from the paper master, it becomes an additional hazard rather than a mitigation. For this reason, the review supports treating the digital layer as a controlled copy whose identity is explicitly bound to the master (shared version identifier, visible "last updated" markers, and auditable revision history). In practice, this creates a governance requirement: owners must be able to demonstrate not only that information exists, but also that it is current, traceable, and resilient to loss of infrastructure.

From a technology standpoint, static PDFs and native apps have practical limitations for rapid decision support. PDFs are easy to distribute but can amplify version divergence and usability issues under stress (scrolling/search, poor progressive disclosure). Native apps can deliver robust offline operation but introduce installation and update barriers, dependence on app stores/MDM policies, and heterogeneous device states across responder organizations. Offline-first PWA solutions can deliver "zero-install" access with controlled caching and versioning—provided that security measures (e.g., CSP/SRI, strict HTTPS, conservative Service Worker design and scope control) and explicit revision governance are implemented. Importantly, PWA adoption should be framed as a trade-off: it reduces deployment friction but requires disciplined handling of cache integrity, update/rollback strategies, and transparent user cues about data currency.

Security considerations further reinforce the need for hybrid redundancy. QR-based entry points are susceptible to replacement and social-engineering attacks ("quishing"), while web delivery introduces integrity and availability risks if trust anchors (domain allow-listing, TLS configuration, and content authenticity checks) are weak. Consequently, operational overlays should minimize the "power" of the QR token (prefer identifiers over full URLs), apply physical hardening, and use user-visible verification steps before loading detailed content. Where confidentiality or sabotage risk is elevated, segmenting Level 1–2 behind an on-site second factor and logging access/changes provides a pragmatic balance between operational value and exposure.

Operationally, success depends less on digitizing the full document and more on prioritizing decision-relevant information in a format compatible with time pressure, limited attention, and degraded physical conditions. The proposed MOD provides a layered framework (Levels 0–2) for progressive disclosure and predictable navigation, reducing cognitive load in the critical early minutes while keeping detailed reference material available when needed. The next step is

 doi:10.20944/preprints202602.1571.v1

operational validation: (i) to identify and standardize the "critical information subset" for Level 0 across building categories and risk profiles, and (ii) to evaluate the hybrid model under realistic constraints (connectivity loss, device variability, glove use, visibility degradation, and deliberate manipulation). Such validation will determine whether the proposed governance and technical safeguards are sufficient in practice and will inform a defensible, implementable specification for hybrid e-FSi deployments.

References

1. Grant, M.J.; Booth, A. A typology of reviews: An analysis of 14 review types and associated methodologies. Health Inf. Libr. J. 2009, 26, 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x.
2. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, n71. https://doi.org/10.1136/bmj.n71.
3. Baethge, C.; Goldbeck-Wood, S.; Mertens, S. SANRA—A scale for the quality assessment of narrative review articles. Res. Integr. Peer Rev. 2019, 4, 5. https://doi.org/10.1186/s41073-019-0064-8.
4. Minister Spraw Wewnętrznych i Administracji. Rozporządzenie z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 poz. 719, z późn. zm.). Available online: https://api.sejm.gov.pl/eli/acts/DU/2010/719/text.pdf (accessed on 14 December 2025).
5. National Fire Protection Association (NFPA). NFPA 1620:2020 Standard for Pre-Incident Planning; NFPA: Quincy, MA, USA, 2020.
6. Li, N.; Yang, Z.; Ghahramani, A.; Becerik-Gerber, B.; Soibelman, L. Situational awareness for supporting building fire emergency response: Information needs, information sources, and implementation requirements. Fire Saf. J. 2014, 63, 17–28. https://doi.org/10.1016/j.firesaf.2013.11.010.
7. European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Off. J. Eur. Union 2014, L 257/73. Available online: https://eur-lex.europa.eu/eli/reg/2014/910/oj (accessed on 10 January 2026).
8. Deutsches Institut für Normung (DIN). DIN 14095:2025-07 Feuerwehrpläne für bauliche Anlagen; DIN: Berlin, Germany, 2025. https://doi.org/10.31030/3621374.
9. Ministère de la Culture (France). Les plans ETARE (plans à destination des services de secours). Available online: https://www.culture.gouv.fr/Thematiques/Monuments-Sites/Intervenir-en-cas-de-sinistre/Les-plans-Eta.-Re. (accessed on 18 January 2026).
10. Royaume de Belgique. Arrêté royal du 28 mars 2014 relatif à la prévention de l'incendie sur les lieux de travail, art. 22 (dossier d'intervention). Available online: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014032818&table_name=loi (accessed on 24 January 2026).
11. Magyarország. 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról (OTSZ). Nemzeti Jogszabálytár. Available online: https://njt.hu/jogszabaly/2014-54-20-0A (accessed on 25 January 2026).
12. Vereinigung zur Förderung des Deutschen Brandschutzes e.V. (vfdb). Technischer Bericht TB 07-01: Leitfaden zur Erstellung von georeferenzierten Feuerwehrplänen; Ausgabe September 2024; vfdb: Germany, 2024. Available online: https://www.vfdb.de/media/doc/technischeberichte/TB_07-01_Technischer_Bericht_georeferenzierte_Feuerwehrplaene.pdf (accessed on 31 January 2026).
13. Service départemental-métropolitain d'incendie et de secours de la Loire (SDIS 42). Guichet sécurité—Plan ETARE (incl. Fiche n°8). Available online: https://www.sdis42.fr/guichet-s%C3%A9curit%C3%A9/formulaire/plan-etare (accessed on 31 January 2026).
14. Service public fédéral (SPF) Emploi, Travail et Concertation sociale (Belgium). Dossier d'intervention incendie (art. 22, AR 28 mars 2014): contenu minimal et modalités. Available online: https://emploi.belgique.be/fr/themes/bien-etre-au-travail/politique-de-prevention/incendie-et-explosion/dossier (accessed on 01 February 2026).
15. Roy, J.M. Preincident Plan Accessibility: An Ongoing Issue; Executive Fire Officer Program Paper; National Fire Academy/FEMA: Emmitsburg, MD, USA, 2010.

 doi:10.20944/preprints202602.1571.v1

16. ISO. ISO 22320:2018 Security and resilience—Emergency management—Guidelines for incident management; ISO: Geneva, Switzerland, 2018.
17. ISO/IEC. ISO/IEC 18004:2024 Information technology—Automatic identification and data capture techniques—QR code bar code symbology specification; ISO: Geneva, Switzerland, 2024.
18. ISO. ISO 23601:2009 Safety identification—Escape and evacuation plan signs; ISO: Geneva, Switzerland, 2009.
19. Rieger, C.; Majchrzak, T.A. Towards the definitive evaluation framework for cross-platform app development approaches. J. Syst. Softw. 2019, 153, 175–199. https://doi.org/10.1016/j.jss.2019.04.001.
20. Harris, M.A.; Brookshire, R.; Chin, A.G. Identifying factors influencing consumers' intent to install mobile applications. Int. J. Inf. Manag. 2016, 36, 441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004.
21. Apple. Distribute managed apps to Apple devices (Apple Platform Deployment). Available online: https://support.apple.com/guide/deployment/ (accessed on 07 February 2026).
22. Google. Manage and distribute apps (Managed Google Play/EMM API). Available online: https://developers.google.com/android/managed-google-play (accessed on 07 February 2026).
23. World Wide Web Consortium (W3C). Service Workers 1; W3C Candidate Recommendation Draft; W3C: 26 January 2026. Available online: https://www.w3.org/TR/service-workers/ (accessed on 08 February 2026).
24. MDN Web Docs. Service Worker API (concepts, lifecycle, offline and caching capabilities). Available online: https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API (accessed on 08 February 2026).
25. Google web.dev. Common techniques to build offline applications (Service Worker caching patterns). Available online: https://web.dev/articles/offline-cookbook (accessed on 08 February 2026).
26. Microsoft. Progressive Web Apps (PWA) documentation (incl. offline-capable patterns and deployment guidance). Available online: https://learn.microsoft.com/en-us/microsoft-edge/progressive-web-apps/how-to/ (accessed on 08 February 2026).
27. ISO. ISO 9241-210:2019 Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems; ISO: Geneva, Switzerland, 2019.
28. Khanlari, P.; Ghasemi, F.; Heidarimoghdam, R. Protective gloves, hand grip strength, and dexterity tests: A comprehensive study. Heliyon 2023, 9, e13592. https://doi.org/10.1016/j.heliyon.2023.e13592.
29. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.2; W3C Recommendation, 2023. Available online: https://www.w3.org/TR/WCAG22/ (accessed on 20 December 2025).
30. World Wide Web Consortium (W3C). Web Content Accessibility Guidelines (WCAG) 2.2: Understanding Success Criterion 2.5.8 Target Size (Minimum); W3C Recommendation, 2023. Available online: https://www.w3.org/TR/WCAG22/#target-size-minimum (accessed on 20 December 2025).
31. Google. Android accessibility: Touch target size (guidelines). Available online: https://support.google.com/accessibility/android/answer/7101858 (accessed on 21 December 2025).
32. Material Design (Google). Accessibility guidance (incl. touch target recommendations). Available online: https://m2.material.io/design/usability/accessibility.html (accessed on 21 December 2025).
33. Endsley, M.R. Toward a theory of situation awareness in dynamic systems. Hum. Factors 1995, 37, 32–64. https://doi.org/10.1518/001872095779049543.
34. Klein, G. Sources of Power: How People Make Decisions; MIT Press: Cambridge, MA, USA, 1998.
35. Sweller, J. Cognitive load during problem solving: Effects on learning. Cogn. Sci. 1988, 12, 257–285. https://doi.org/10.1207/s15516709cog1202_4.
36. Shneiderman, B. The eyes have it: A task by data type taxonomy for information visualizations. In Proceedings of the 1996 IEEE Symposium on Visual Languages; IEEE: Washington, DC, USA, 1996; pp. 336–343. https://doi.org/10.1109/VL.1996.545307.
37. Pirolli, P.; Card, S. Information foraging in information access environments. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '95); ACM: New York, NY, USA, 1995; pp. 51–58. https://doi.org/10.1145/223904.223911.

 doi:10.20944/preprints202602.1571.v1

38. Pirolli, P.; Card, S. Information foraging. Psychol. Rev. 1999, 106, 643–675. https://doi.org/10.1037/0033-295X.106.4.643.
39. Jones, W.W.; Holmberg, D.G.; Davis, W.D.; Bushby, S.T.; Reed, K.A. Workshop to Define Information Needed by Emergency Responders During Building Emergencies; NISTIR 7193; NIST: Gaithersburg, MD, USA, 2005. https://doi.org/10.6028/NIST.IR.7193.
40. Holmberg, D.G.; Raymond, M.A.; Averill, J.D. Delivering Building Intelligence to First Responders; NIST Technical Note 1648; NIST: Gaithersburg, MD, USA, 2013. https://doi.org/10.6028/NIST.TN.1648.
41. Averill, J.D.; Holmberg, D.G.; Vinh, A.B.; Davis, W.D. Building Information Exchange for Fire Responders Workshop: Proceedings; NIST Technical Note 1643; NIST: Gaithersburg, MD, USA, 2010.
42. Seppänen, H.; Mäkelä, J.; Luokkala, P.; Virrantaus, K. Developing shared situational awareness for emergency management. Saf. Sci. 2013, 55, 1–9. https://doi.org/10.1016/j.ssci.2012.12.009.
43. National Fire Protection Association (NFPA). NFPA 1660:2024 Standard for Emergency, Continuity, and Crisis Management: Preparedness, Response, and Recovery; NFPA: Quincy, MA, USA, 2024.
44. National Fire Protection Association (NFPA). NFPA 170:2024 Standard for Fire Safety and Emergency Symbols; NFPA: Quincy, MA, USA, 2024.
45. Okoli, J.O.; Weller, G.; Watt, J. Information processing and intuitive decision-making on the fireground: The role of working memory, situation awareness, and experience. Cogn. Technol. Work 2016, 18, 89–103. https://doi.org/10.1007/s10111-015-0348-9.
46. Rezaeifam, S.; Ergen, E.; Günaydın, H.M. Fire emergency response systems information requirements' data model for situational awareness of responders: A goal-directed task analysis. J. Build. Eng. 2023, 63, 105531. https://doi.org/10.1016/j.jobe.2022.105531.
47. ISO. ISO 7010:2019 Graphical symbols—Safety colours and safety signs—Registered safety signs; ISO: Geneva, Switzerland, 2019.
48. Vidas, T.; Owusu, E.; Wang, S.; Zeng, C.; Cranor, L.F.; Christin, N. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In Financial Cryptography and Data Security (FC 2013); Sadeghi, A.-R., Ed.; LNCS 7862; Springer: Berlin/Heidelberg, Germany, 2013; pp. 52–69. https://doi.org/10.1007/978-3-642-41320-9_4.
49. Kieseberg, P.; Leithner, M.; Mulazzani, M.; Munroe, C.; Schrittwieser, S.; Sinha, A.; Weippl, E.R. QR code security: A survey of attacks and challenges for usable security. In Human Aspects of Information Security, Privacy, and Trust (HAS 2014); Tryfonas, T., Askoxylakis, I., Eds.; LNCS 8533; Springer: Cham, Switzerland, 2014; pp. 79–90. https://doi.org/10.1007/978-3-319-07620-1_8.
50. Sharevski, F.; Devine, A.; Pieroni, E.; Jachim, P. Phishing with malicious QR codes. In Proceedings of the European Symposium on Usable Security (EuroUSEC 2022), Rennes, France, 18 April 2022; ACM: New York, NY, USA, 2022; pp. 160–171. https://doi.org/10.1145/3549015.3554172.
51. Kumar, N.; Jain, S.; Kaulgud, V. How safe is QR code? Understanding user awareness and perception toward QR code security. In HCI International 2022; Springer: Cham, Switzerland, 2022. https://doi.org/10.1007/978-3-031-06394-7_64.
52. Cybersecurity and Infrastructure Security Agency (CISA). Phishing Guidance: Stopping the Attack Cycle at Phase One; CISA: Washington, DC, USA, 2023. Available online: https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one (accessed on 27 December 2025).
53. U.S. Department of Health and Human Services (HHS); Health Sector Cybersecurity Coordination Center (HC3). QR Codes and phishing as a threat to the HPH Sector; HC3: Washington, DC, USA, 2023. Available online: https://www.hhs.gov/sites/default/files/qr-codes-and-phishing-as-a-threat-to-the-hph-white-paper.pdf (accessed on 27 December 2025).
54. Federal Bureau of Investigation (FBI); Internet Crime Complaint Center (IC3). North Korean Kimsuky Actors Leverage Malicious QR Codes in Spearphishing Campaigns Targeting U.S. Entities; FLASH Report No. CP-000111-MW; 8 January 2026. Available online: https://www.ic3.gov/CSA/2026/260108.pdf (accessed on 14 February 2026).
55. ISO/IEC. ISO/IEC 20248:2018 Information technology—Automatic identification and data capture techniques—Data structures for barcode and two-dimensional symbol authenticity and traceability; ISO: Geneva, Switzerland, 2018.

56. El-Ansari, A.; Hallynck, M.; Lison, P. Quick Response Code Secure: A Cryptographically Secure Anti-Phishing and Anti-Tampering Client-Server Based Solution. In Information Systems Security and Privacy (ICISSP 2018); Springer: Cham, Switzerland, 2018. https://doi.org/10.1007/978-3-319-65127-9_25.
57. Focardi, R.; Luccio, F.L.; Wahsheh, H.A.M. Usable Cryptographic QR Codes. In Proceedings of the 2018 IEEE International Conference on Industrial Technology (ICIT 2018), Lyon, France, 20–22 February 2018; IEEE: Piscataway, NJ, USA, 2018. https://doi.org/10.1109/ICIT.2018.8352431.
58. Chinprutthiwong, P.; Vardhan, R.; Yang, G.; Zhang, Y.; Gu, G. The service worker hiding in your browser: The next web attack target? In Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2021), San Sebastián, Spain, 6–8 October 2021; ACM: New York, NY, USA, 2021; pp. 312–323. https://doi.org/10.1145/3471621.3471845.
59. Chinprutthiwong, P.; Vardhan, R.; Yang, G.; Gu, G. Security study of service worker cross-site scripting. In Proceedings of the Annual Computer Security Applications Conference (ACSAC 2020), Virtual Event, 7–11 December 2020; ACM: New York, NY, USA, 2020; pp. 643–654. https://doi.org/10.1145/3427228.3427290.
60. Karami, S.; Ilia, P.; Polakis, J. Awakening the Web's sleeper agents: Misusing service workers for privacy leakage. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2021), Virtual Event, 21–25 February 2021; Internet Society: Reston, VA, USA, 2021. https://doi.org/10.14722/ndss.2021.23104.
61. Nguyen, H.V.; Iacono, L.L.; Federrath, H. Your cache has fallen: Cache-poisoned denial-of-service attack. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2019), London, UK, 11–15 November 2019; ACM: New York, NY, USA, 2019; pp. 1915–1936. https://doi.org/10.1145/3319535.3354215.
62. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). Off. J. Eur. Union 2016, L 119/1. Available online: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679 (accessed on 11 January 2026).
63. European Union. Directive (EU) 2022/2555 (NIS2 Directive). Off. J. Eur. Union 2022, L 333/80. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (accessed on 11 January 2026).
64. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025; ENISA: Athens/Heraklion, Greece, 2025. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed on 15 February 2026).
65. Souppaya, M.; Kent, K. Guide to Computer Security Log Management; NIST Special Publication 800-92; NIST: Gaithersburg, MD, USA, 2006. https://doi.org/10.6028/NIST.SP.800-92.
66. Reason, J. Human error: Models and management. BMJ 2000, 320, 768–770. https://doi.org/10.1136/bmj.320.7237.768.
67. Tissington, P.A.; Flin, R. Assessing risk in dynamic situations: Lessons from fire service operations. Risk Manag. 2005, 7, 43–51. https://doi.org/10.1057/palgrave.rm.8240226.
68. Steen-Tveit, K.; Munkvold, B.E. From common operational picture to common situational understanding: An analysis based on practitioner perspectives. Saf. Sci. 2021, 142, 105381. https://doi.org/10.1016/j.ssci.2021.105381.
69. Bharosa, N.; Lee, J.; Janssen, M. Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. Inf. Syst. Front. 2010, 12, 49–65. https://doi.org/10.1007/s10796-009-9174-z.
70. Bunker, D.; Levine, L.; Woody, C. Repertoires of collaboration for common operating pictures of disasters and extreme events. Inf. Syst. Front. 2015, 17, 51–65. https://doi.org/10.1007/s10796-014-9515-4.
71. Weidinger, J.; et al. Determinants for the acceptance of emergency response information systems: Analyses with German firefighters. Int. J. Disaster Risk Reduct. 2024, 109, 104603. https://doi.org/10.1016/j.ijdrr.2024.104603.