primion

Integration Before Resilience

Why Converged Operations Decide Who Survives a Crisis and Who Discovers Their Fragmentation Too Late

Position Paper

Francis Cepero, Group CEO, Primion

TABLE OF CONTENTS

This paper accompanies Primion's keynote at ASIS Europe 2026 in Antwerp, Belgium, "From Access Control to Workforce Advantage: Redesigning Security for the Human Era." It deepens the questions raised in that presentation and proposes a structural framework for evaluating resilience architectures. The argument draws on documented crisis failures, enterprise integration patterns observed in active procurement processes, and operational evidence from critical infrastructure operators managing hundreds of thousands of identities across multiple countries.

The Pattern:

Coordination Fails Systematically at the Same Structural Point

01

1. The Pattern: Coordination Fails Systematically at the Same Structural Point

On 29 October 2024, the Spanish region of Valencia experienced catastrophic flooding. Meteorological services had issued severe rainfall warnings five days before the event. On the morning of the catastrophe, a red alert was active by 07:36. Rivers and ravines began overflowing upstream before noon. The first fatality was recorded by midday. Yet the regional crisis center issued no public alert until 20:30 that evening, advising residents to move to upper floors. By that point, entire neighborhoods were already submerged. Many of the 237 victims died trying to retrieve their cars from underground garages, unaware of the danger until water reached their streets. Total damage exceeded EUR 10.7 billion.

The monitoring systems worked. The meteorological data was accurate. The river gauges reported correctly. **What failed was the coordination between these systems and the decision to act.** Information existed in one place. Authority existed in another. Communication capacity to the public existed in a third. No integration layer connected them.

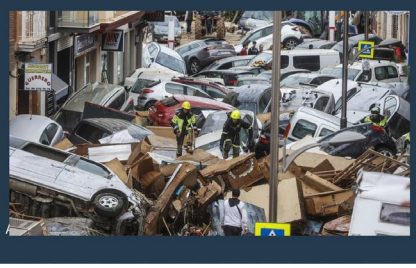
It should be noted that the delay in Valencia was not purely a technology failure. The decision to withhold public alerts reflected governance failures and institutional incentive structures that no integration platform can override. What integration can do is eliminate the excuse that information was not available or not connected. It makes the decision to act or not to act a visible, accountable choice rather than an invisible default.

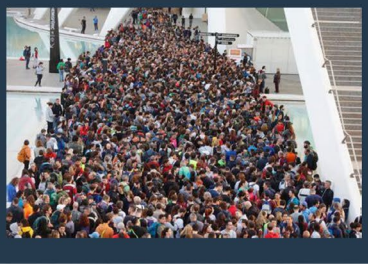
Valencia 29.10.2024: All signals were there, but lack of integration failed to produce a coordinated response

The cascade from prediction to catastrophe: **> 220 avoidable deaths - 10.7 € bln destruction**

5 days before	12 hours before	6 hours before	20:30	Days after
No public announcement	*No public announcement*	*No public announcement*	*Public Announcement*	
Weather prediction available	Flood warnings issued	Higher cities flooded No evacuation	"Move upstairs" 100+ already dead	Volunteers self-organize Poor coordination

Integration and coordination failures, not weather, were the root causes.





A different kind of failure, smaller in scale but identical in structure, played out at Munich Airport during winter operations. Heavy snowfall disrupted ground handling. Six hundred passengers spent the night stranded on aircraft because operations could not mobilize bus drivers to transport them to the terminal. The drivers had gone home. The operations center had no phone numbers, no real-time availability data, and no access to an external standby pool. The scheduling system had done its job: shifts had been planned, hours had been recorded. But when the situation required reaching actual people in real time, the system had nothing to offer.

These are not isolated failures. They are instances of a structural pattern that repeats across geographies, industries, and crisis types. Large organizations invest heavily in domain-specific systems: access control, surveillance, IT security, workforce scheduling, operational technology monitoring. Each system functions within its own domain. But no integration layer connects visibility across domains to coordinated decision-making and action. The technology works. The coordination between technologies does not.

This pattern is now visible in procurement as well. Large European multinationals have begun issuing requests for information that span IT security, OT security, physical security, identity management, and workforce management in a single document. These RFIs demand observability, converged security operations, and real-time workforce coordination as integrated capabilities. Traditional security vendors, specialists in one domain, cannot respond to these documents because the questions themselves cross every boundary their products were designed to respect.

The structural prerequisite for resilience is not better individual systems. It is integration across systems, domains, and organizational boundaries.

The Mechanism:

How Crises Evolve Faster Than Fragmented Institutions Can Adapt

02

2. The Mechanism: How Crises Evolve Faster Than Fragmented Institutions Can Adapt

Understanding why coordination fails requires understanding how crises actually behave. The Cynefin framework, developed by Dave Snowden and widely adopted in crisis management and organizational theory, distinguishes four domains of situational complexity. In the simple domain, the relationship between cause and effect is obvious, and a standard operating procedure suffices. In the complicated domain, cause and effect require expert analysis. In the complex domain, cause and effect can only be perceived in retrospect, and the appropriate response is to probe, sense, and adapt. In the chaotic domain, no causal relationship is discernible at the system level, and the only viable response is to act first and impose order through intervention.

Real crises do not stay in one domain. They evolve through phases, often in hours.

The Valencia timeline maps precisely onto this progression. The forecast phase was complicated: expert meteorological analysis was available, and the appropriate response would have been structured preparation. What happened instead was bureaucratic monitoring and institutional blame-shifting. The flood onset was complex: conditions on the ground were changing rapidly, upstream and downstream effects were interacting unpredictably, and the appropriate response would have been rapid local adaptation. What happened instead was slow escalation through hierarchical approval chains. The catastrophic flooding phase was chaotic: entire cities were submerged, 15,000 emergency calls overwhelmed the 112 system, and the appropriate response would have been immediate mass alert and population-level action. What happened instead was a delayed decision issued nine hours too late.

The aftermath revealed a fourth failure. Disaster recovery required coordinated mobilization of cleanup crews, temporary shelter, logistics, and volunteer management. Thousands of volunteers traveled to Valencia from across Spain. Public solidarity moved faster than institutional coordination. Volunteers self-organized because no system existed to direct them, assign them tasks, or even register their presence. The crisis had moved from chaotic back through complex to complicated, but the institutional response never caught up.

This is not a uniquely Spanish problem. The same phase evolution applies to cyberattacks that escalate from an initial breach through lateral movement to operational disruption. It applies to industrial incidents where a localized failure cascades across interdependent systems. It applies to any scenario where the speed of the crisis exceeds the speed of institutional decision-making. And in every case, the bottleneck is the same: fragmented systems cannot provide the real-time, cross-domain visibility that each phase transition demands.

The Requirement:

What a Converged Operations Architecture Must Actually Deliver

03

3. The Requirement: What a Converged Operations Architecture Must Actually Deliver

If the problem is structural fragmentation, and if crises demand real-time coordination across domains, then the requirement for any serious resilience architecture becomes clear. It is not another point solution. It is a converged operations layer that unifies four domains under a shared identity and integration fabric.

The first domain is workforce operations.

Any organization that cannot answer the question "who is on site right now, and are they qualified for what they are doing?" is not resilient; it is merely lucky. Workforce operations must provide real-time visibility into the location, availability, and qualifications of all workers, whether permanent or temporary, internal or external, frontline or back-office. This includes demand forecasting, flexible shift scheduling, same-day adjustments, and the ability to mobilize replacements from internal and external pools within minutes, not hours. The Munich Airport failure was a workforce operations failure. The Valencia disaster recovery was a workforce operations failure at regional scale.

The second domain is access and identity.

The Valencia crisis demonstrated that knowing who is authorized to be where, and being able to verify that in real time, is not an administrative convenience but an operational prerequisite: emergency responders, institutional actors, and volunteers all needed to be identified, directed, and coordinated, and no shared identity layer existed to do so. Large enterprises face the same challenge in peacetime: a single critical infrastructure operator may manage 250,000 employees, 25,000 access readers, and multiple access control vendors across dozens of sites. The identity plane must cover not only employees in the HR system of record but also contractors, temporary workers, visitors, and increasingly, machines and AI agents that interact with physical and digital systems. Access policies must be enforceable based on qualifications, shift assignments, and real-time context, not merely based on static role assignments. Without a unified identity layer, every other coordination capability is built on sand.

The third domain is converged security across IT, OT, and physical systems.

In Valencia, weather monitoring, river gauges, emergency communication, and civil protection operated as separate signal chains with no shared intelligence layer. The same fragmentation exists inside enterprises: a login into a programmable logic controller on the factory floor, a door opening in a restricted area, and a network authentication in the data center are three expressions of the same question: is this entity authorized to perform this action at this time in this place? When these three signals are processed by three separate systems with no shared context, anomalies that span domains become invisible. A contractor who badges into a building after

hours and simultaneously authenticates to an OT network is a pattern that no single-domain system can detect. Converged security means shared observability, shared intelligence, and coordinated response across all three layers.

The fourth domain is threat detection and compliance.

The Cynefin analysis in Section 2 showed that crises transition between phases at speeds that overwhelm periodic reporting cycles. This applies equally to compliance and threat detection: anomaly detection, critical event management, and regulatory compliance must operate on the same data and coordination fabric as normal operations. Compliance that exists only in periodic reports cannot contribute to real-time resilience. Threat detection that operates in a security operations center disconnected from workforce and access data cannot correlate the signals that matter most.

These four domains cannot be unified by placing a dashboard on top of four separate products. The convergence must happen at the identity and data level. A “single pane of glass” that aggregates views from disconnected systems is a visualization layer, not an integration layer. It will show you the crisis. It will not help you coordinate the response.

The requirement profile, then, is a platform that shares a single identity model across all four domains, integrates southbound with the full heterogeneity of existing hardware and software (multiple access control vendors, multiple OT systems, multiple enterprise platforms), and provides northbound integration into business processes, critical event management, and observability. This is not a theoretical construct. It is what current enterprise RFIs are demanding, in increasing specificity, from their security and workforce management suppliers.

The Proof:
Converged Operations in Production, at Scale

04

4. The Proof: Converged Operations in Production, at Scale

Architecture requirements are easy to articulate. Operational proof is harder. The question for any organization evaluating its resilience posture is not whether converged operations sounds appealing but whether anyone has actually built it, deployed it at enterprise scale, and operated it over years.

Frankfurt Airport offers one answer. Fraport, the operator of Frankfurt Airport, has maintained a converged security and workforce management partnership with Primion for eighteen years, a partnership that has been continuously modernized through four platform generations while maintaining uninterrupted operations. The operational scope is instructive: 60 million passengers annually served through 612 gate management terminals, 23,000 employees across 178 gates with integrated time and attendance, 81,000 managed identities from 70 nations with access authorizations across 4,302 readers, and 75,000 managed ID cards covering both people and transport vehicles. This is not a pilot. It is converged operations at the scale of a small city, running in production, with the kind of operational continuity that only sustained integration can deliver.

A large European critical infrastructure operator, publicly referenced in industry contexts, presents an even more complex case: 250,000 employees, 25,000 readers, and a heterogeneous landscape of access control vendors accumulated through decades of organic growth and acquisition. The integration challenge is not greenfield deployment but harmonization: bringing multiple generations of hardware, multiple vendor ecosystems, and multiple organizational cultures under a single converged operations platform while maintaining uninterrupted service.

These cases demonstrate that the requirement profile derived in the previous section is not aspirational. It is operational. The technology to unify workforce operations, access and identity, converged IT/OT/physical security, and threat management under a shared identity layer exists, is deployed, and is proven at scales that exceed what most organizations will ever require.

Conclusion

The question is not whether your organization has invested in security. It almost certainly has. The question is whether your security, workforce, identity, and operational technology systems can coordinate in real time when a crisis moves faster than your institutional processes. Valencia demonstrated what happens when they cannot. The organizations that will define the next standard of resilience are not those with the most security technology. They are those that integrated first.

The challenge ahead will intensify. Today, organizations coordinate people, permissions, and processes. Tomorrow, they will coordinate people, autonomous machines, and AI agents, at scales that make today's complexity look modest. The architectural decision to converge now is not only a response to current failures. It is preparation for a future in which fragmented systems will not merely underperform. They will be ungovernable.

To learn more or discuss how the converged operations framework applies to your organization, contact us at resilienceadprimion.eu or visit primion.eu

References

Institutional and Governmental

- Generalitat Valenciana, DANA crisis timeline and emergency response documentation, October-November 2024
- European Commission, EU Civil Protection Mechanism activation reports, Valencia flooding, 2024
- Levante EMV, “Cronica 2024: El ano de la DANA mortal,” 31 December 2024

Industry and Operational

- ASIS International, ASIS Europe 2026 conference program, Barcelona
- Fraport AG, Frankfurt Airport operational statistics, 2024-2025
- Aviation Source News, “Munich Airport apologises after 600 passengers spend night stranded on aircraft due to snow,” 2025

Frameworks and Academic

- Snowden, D.J. and Boone, M.E., “A Leader’s Framework for Decision Making,” Harvard Business Review, November 2007
- Primion Technology AG, Converged Security Operations reference architecture documentation, 2025-2026

primion

Primion Technology GmbH
Steinbeisstr. 2–5 | 72510 Stetten am kalten Markt | Germany
Tel. +49 7573 9520 | info@primion.de | primion.io