

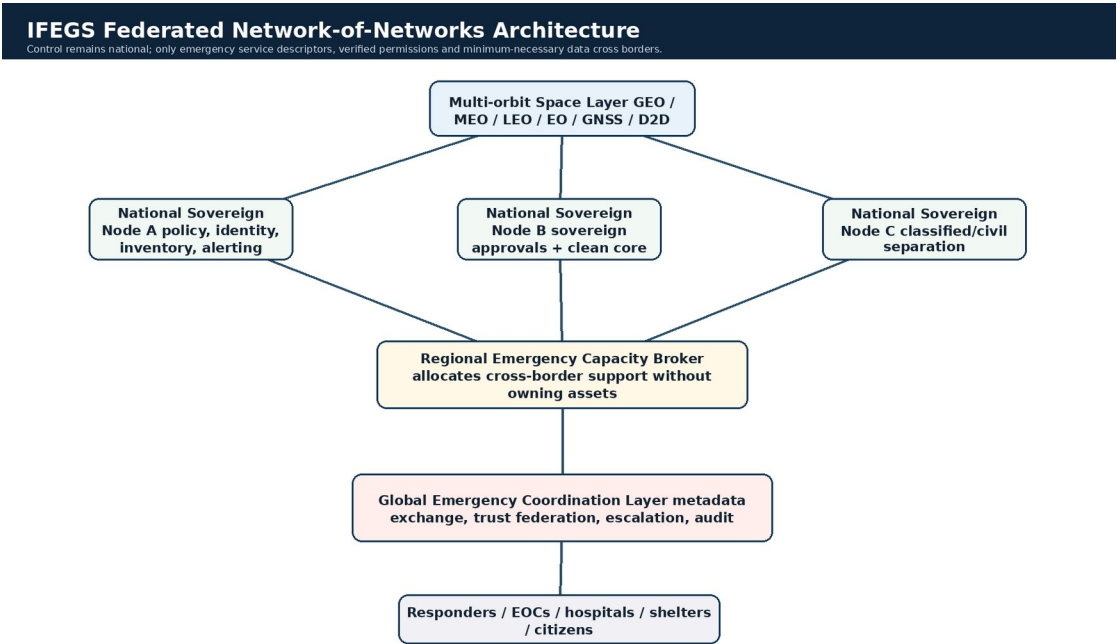
INTERNATIONAL FEDERATED EMERGENCY GROUND SEGMENT

IFEGS

Master Integrated Manuscript

Contingency Plan • Technical Reference Architecture • Cyber-Resilient Failover • Institutional Implementation

A federated global-regional-national framework for resilient satellite ground-segment interoperability during disasters, cyber incidents and security crises.



Institutional Working Draft | September 2026

Prepared for technical review by space, telecommunications, civil-protection, cybersecurity and security stakeholders

Document Purpose and Status

Purpose. This integrated manuscript provides a technically detailed contingency and reference architecture for cross-network ground-station interoperability, autonomous but bounded failover, secure crisis-data exchange and multinational emergency coordination.

Status. Institutional working draft for technical, regulatory, legal and operational review. It is structured so that individual modules may later be converted into standards, implementation profiles, model agreements, test plans and regional pilots.

CORE PROPOSITION

Do not create one global controller of all ground stations. Create a federated network-of-networks in which sovereign national nodes retain authority, regional brokers coordinate capacity, and a global layer exchanges only the minimum trusted metadata required for emergency interoperability.

Intended Institutional Users

- National and regional space agencies and satellite operators
- Telecommunications regulators, mobile-network operators and satellite-service providers
- Civil-protection, disaster-management and humanitarian organizations
- Cybersecurity authorities, SOC/NOC operators and critical-infrastructure owners
- International standardization, policy, legal and security institutions

How to Use This Manuscript

Decision-makers can begin with the Executive Summary, Parts I, IV and VII. **Systems engineers** should focus on Parts II, III, V and VI. **Legal and policy teams** should focus on the governance, legal framework, operating model and annexes.

Contents

PART I | Foundations & Federated Architecture

Executive Summary; 1. Problem Definition and Scope; 2. State of the Art; 3. Design Principles; 4. Proposed IFECS Architecture

PART II | Space-Ground & Ground-Ground Communications

5. Technical Architecture of Space-Ground Communications; 6. Ground-to-Ground Interconnection Between Stations

PART III | Failover, Cybersecurity & Data Assurance

7. Autonomous Failover; 8. Cybersecurity and Cyberattack Contingency; 9. Secure Database and Information Exchange; 10. Human Factors

PART IV | Crisis Scenarios, Governance & Law

11. Concrete Crisis Scenarios; 12. Strategic Architecture and Governance; 13. Legal and Regulatory Framework; 14. Emerging Technologies

PART V | Standards, Roadmap & Technical Annexes

15. Missing Gaps; 16. Recommended Standards Family; 17. Implementation Roadmap; 18. 24-Hour Activation Checklist; 19-22. Technical Annexes

PART VI | Detailed Engineering & Institutionalization

23. Detailed Satellite-Ground Engineering; 24. Ground-Ground Connectivity; 25. Multi-Orbit Integration; 26. Cyber-Physical Playbooks; 27-34. Regional, institutional, policy and implementation chapters

PART VII | Supplementary Institutional Annexes

Annex D. Expanded Threat Model; Annex E. Global/Regional/National Operating Model; Annex F. Japan-Type Earthquake and Tsunami Scenario; Annex G. Expanded Legal Framework; Annex H. Working Group Decision Package; Annex I. Conformance Levels

Note: section numbering is intentionally retained to support later standardization, cross-reference and institutional review workflows.

Executive Summary

Decision-level message: The required capability is not a new global constellation or a centralized super-network. It is a trusted federation layer that can discover compatible services, authorize emergency use, reroute traffic across independent networks, protect sovereign data and continue minimum life-safety services under degraded trust.

This manuscript proposes a contingency architecture for federating satellite ground stations, terrestrial telecommunications nodes, emergency operations centres and disaster data systems during catastrophic events. The purpose is to move beyond the current model in which emergency connectivity is restored through ad hoc deployment of terminals, manual coordination and operator-by-operator agreements. The proposed International Federated Emergency Ground Segment, or IFECS, is designed as a network-of-networks: nationally controlled, regionally coordinated and globally interoperable without creating a single centralized global control point.

The design problem is not only technical. During a major earthquake, flood, wildfire, cyclone, geopolitical crisis or cyberattack, the question is not simply whether a satellite exists or whether a ground station exists. The real question is whether a trusted actor can discover available capacity, verify compatibility, obtain legal permission, allocate priority, route traffic through a clean path, protect sensitive databases, preserve evidence and restore service without introducing new strategic vulnerabilities.

The central conclusion is that the most convenient and realistic recommendation is not to build a new monolithic global ground-station network. The recommended approach is a federated service architecture using standardized emergency service descriptors, strong identity, pre-negotiated legal clauses, regional capacity brokers, sovereign national nodes, zero-trust database access, bounded autonomous failover and clean-core cyber-resilient operational modes.

- Ground stations should expose emergency services through standardized descriptors rather than full internal system access.
- National authorities should retain sovereignty over assets, spectrum, classified data and public warning decisions.
- Regional emergency capacity brokers should coordinate multi-country routing, spare capacity, terminals, gateway access and conflict resolution.
- A global emergency coordination layer should exchange metadata, trust status, escalation requests and audit records, not bulk sensitive data.
- Autonomous failover should be permitted only inside pre-authorized envelopes; cross-border, command-link, classified and destructive actions require human authorization.
- Databases should remain modular and sovereign, accessed through policy-controlled query interfaces, cross-domain guards and time-limited emergency tokens.
- Cyberattack response must be designed as a primary operating mode, not as an annex.

PART I

FOUNDATIONS & FEDERATED ARCHITECTURE

Scope, state of the art, design principles and the five-tier IFEKS federation model.



1. Problem Definition and Scope

Modern disaster response depends on space-enabled communications, Earth observation, GNSS timing and positioning, weather data, telecommunications infrastructure, public alerting and secure data exchange. However, these systems remain fragmented across satellite operators, ground-station owners, public agencies, armed forces, civil protection bodies, humanitarian organizations and commercial network providers. In a catastrophe, the fragmentation becomes operationally visible: several functioning networks may exist, yet organizations cannot always interoperate quickly enough.

Ground stations are usually optimized for specific missions, frequency bands, waveforms, security domains, regulatory authorizations and operational procedures. Many stations can support cross-support services, but few can automatically accept a heterogeneous emergency workload from another operator or country without technical, legal and security preconditions. The proposed contingency plan addresses these bottlenecks by treating the ground segment as a federated emergency utility while preserving sovereign and commercial control.

1.1 Working definition

For this manuscript, “ground segment” includes fixed satellite ground stations, teleports, TT&C stations, mission control networks, satellite gateways, portable VSATs, mobile emergency gateways, 4G/5G core and radio access nodes, public-safety communications nodes, microwave/fibre backhaul, edge data centres, database interfaces, operations centres and secure routing overlays. The architecture therefore covers both space-ground communications and ground-ground interconnection between stations and institutions.

1.2 Event classes covered

Event class	Examples	Ground-segment stressor	Primary IFECS response
Climate disaster	Mega-floods, cyclones, wildfire smoke, extreme heat	Power loss, flooded stations, damaged fibre, massive public warning demand	Multi-orbit backup, D2D alerts, regional capacity, portable edge nodes
Geophysical disaster	Earthquakes, tsunamis, volcanic eruption	Station damage, road/airport closure, tower collapse	Pre-authorized failover to unaffected stations, DTN, mobile gateways
Cyber crisis	Ransomware, destructive malware, credential theft, supply-chain compromise	Loss of trust in network/control path	Clean core, trust revocation, staged re-entry, segmented routing
Hybrid/security crisis	Jamming, spoofing, cyber disruption, kinetic infrastructure threat	Contested RF spectrum and sensitive data boundaries	Civil/security separation, protected services, sovereign authorization
Public health or mass displacement	Pandemic, refugee flow, shelter overload	Demand surge, identity and logistics data needs	Secure database federation and priority communications

2. State of the Art: Capabilities to Build Upon

The proposed plan intentionally uses existing capabilities where possible. The value of IFECS is not the invention of a new waveform or a new satellite constellation, but the integration of existing and emerging capabilities into an operationally credible contingency framework. The following capabilities are already relevant.

Capability	Current maturity	Role in IFECS	Limitation to solve
GEO satellite communications	Mature	Wide-area resilient services, broadcast warning, government networks	Latency, weather attenuation, terminal availability
MEO broadband	Mature/emerging	Lower-latency resilient trunking and emergency backhaul	Gateway and terminal availability

Capability	Current maturity	Role in IFECS	Limitation to solve
LEO broadband	Operational and expanding	Rapid deployable broadband, resilient backhaul, rural coverage	Gateway dependence, capacity, regulatory permission
Direct-to-device satellite / NTN	Emerging rapidly	Citizen alerting and basic connectivity when cellular fails	Capacity, handset compatibility, roaming and priority rules
CCSDS SLE/CSTS cross support	Mature standards family	Mission cross-support and station service abstraction	Not universally implemented or operationalized for emergency brokerage
DTN / BPv7	Standards-based, operational in space contexts	Store-and-forward across intermittent links and damaged infrastructure	Needs terrestrial emergency integration and operations training
CAP alerting	Mature standard	Consistent multi-channel public warnings	Requires local authority, language, trust and dissemination integration
Zero Trust / HSM / PKI	Mature cybersecurity practices	Federated identity, credential revocation, access control	Needs emergency-specific trust profiles and sovereignty rules
AI/automation	Rapidly advancing	Anomaly detection, routing recommendations, contact scheduling	Must be bounded, auditable and human-supervised

Relevant reference foundations include the CCSDS cross-support family for standardized space link services; the IETF Bundle Protocol version 7 for disruption-tolerant networking; OASIS Common Alerting Protocol version 1.2 for all-hazard public warning; ITU emergency telecommunications frameworks, including the Tampere Convention and Resolution 647; 3GPP non-terrestrial network work for satellite integration with mobile systems; and national/regional cybersecurity frameworks such as NIS2 for critical infrastructure.

3. Design Principles

Principle	Meaning	Design implication
Federation over centralization	No single global controller of all ground stations	Use national nodes, regional brokers and global metadata exchange
Sovereignty by design	States retain control over assets, spectrum, command and sensitive data	Route requests through national sovereign authorization gates
Minimum necessary data	Do not replicate national databases into a global repository	Use metadata catalogues, controlled queries and purpose-bound tokens
Fail-safe autonomy	Automation may accelerate safe operations but must not create uncontrolled escalation	Bounded failover envelopes, human-in-the-loop thresholds
Clean-core resilience	A compromised network must not poison the emergency network	Pre-hardened, isolated services with independent identity and logs
Multi-orbit and multi-bearer diversity	No single constellation, station, frequency band or terrestrial route is sufficient	PACE routing across GEO/MEO/LEO/D2D/fibre/microwave/public safety radio
Auditability	Every emergency action must be traceable after the event	Immutable logs, evidence chains, non-repudiation and after-action review
Legal pre-clearance	Emergency is not the time to negotiate every permission	Pre-negotiated clauses, spectrum procedures, model MOUs and SLAs

4. Proposed IFEGS Architecture

IFEGS is composed of five tiers. The architecture is deliberately modular: a country or region can implement one tier first and expand later. The minimum viable deployment is a national sovereign node with a station registry, trust service, PACE routing playbook and connection to at least one regional broker.

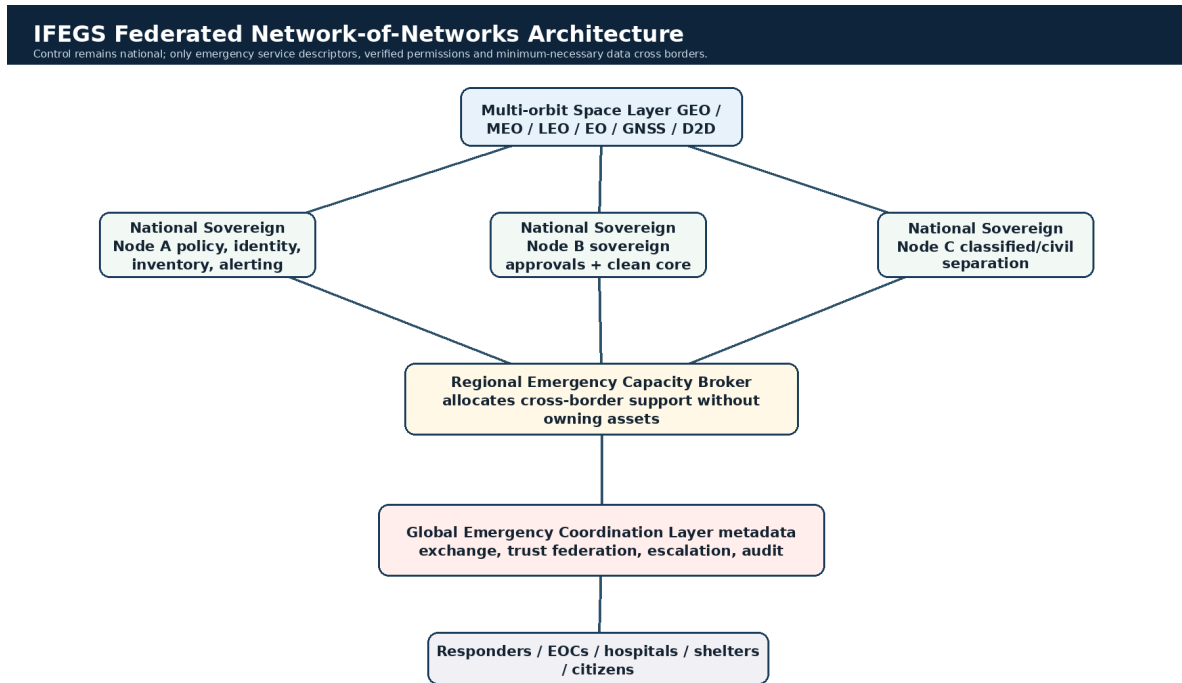


Figure 2. IFEGS federated architecture: national control, regional brokerage and global coordination.

4.1 Tier 0: asset layer

The asset layer contains the physical and logical communications resources: antennas, RF chains, modems, baseband equipment, mission control systems, satellite gateways, teleports, public-safety networks, cellular networks, IP/MPLS routers, emergency terminals, mobile gateways, drones, HAPS platforms and edge compute nodes.

4.2 Tier 1: station service adapter

Each participating station deploys a station service adapter. The adapter does not expose the internal mission network. Instead, it publishes a controlled service interface describing what emergency services the station can provide. Examples include telemetry reception, telecommand forwarding under strict authorization, IP backhaul, public alert broadcast, EO data downlink, storage relay, DTN bundle forwarding, gateway hosting or protected voice/data services.

4.3 Tier 2: national sovereign node

The national node is the legal and operational authority layer. It validates domestic assets, maintains the national ground-station registry, holds national emergency priority policies, manages domestic identity trust, authorizes cross-border support, controls sensitive data exposure and coordinates with telecom regulators and civil protection agencies.

4.4 Tier 3: regional emergency capacity broker

The regional broker coordinates demand and available capacity across countries in a region. It does not command national assets directly. It receives requests, evaluates compatible services, applies pre-agreed regional rules, recommends routing, resolves capacity conflicts and escalates legal/security exceptions. Regional brokers are

particularly important for flood basins, seismic zones, island regions and security environments where disasters cross borders.

4.5 Tier 4: global emergency coordination layer

The global layer provides global situational awareness, inter-regional escalation, trust status exchange, catalogue synchronization, audit anchors, exercise coordination and minimum emergency service interoperability. It should be distributed and multi-hosted across trusted international organizations and participating regions rather than implemented as a single global operations centre.

PART II

SPACE-GROUND & GROUND-GROUND COMMUNICATIONS

RF, link, transport and station-service interoperability across heterogeneous satellite and terrestrial infrastructures.



5. Technical Architecture of Space-Ground Communications

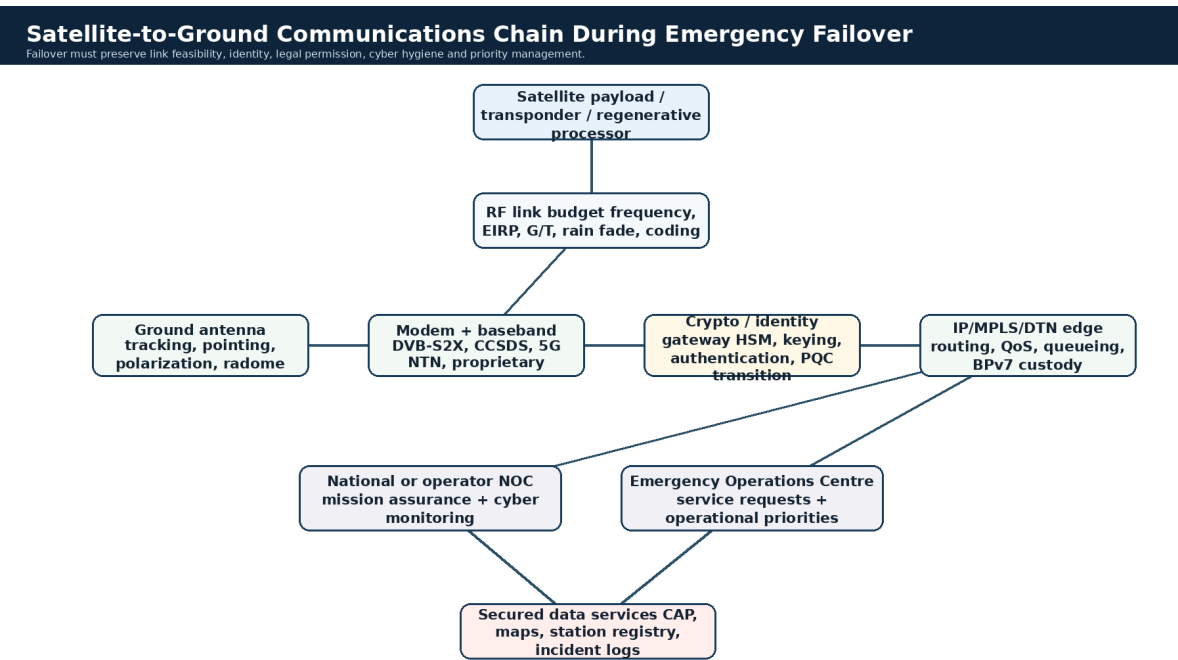


Figure 3. Satellite-to-ground communication chain and failover checkpoints.

A ground-segment contingency plan must understand the complete satellite-to-ground chain. The emergency path is only as strong as its weakest component. A satellite may be healthy, but service may fail because of antenna pointing loss, rain attenuation, modem incompatibility, expired keys, backhaul fibre disruption, power failure, spectrum authorization, compromised identity, congested queues or the absence of a legal routing agreement.

5.1 RF and physical layer

The physical layer includes frequency band, polarization, modulation, coding, antenna gain, tracking accuracy, availability target, rain fade margin, site diversity, EIRP, G/T, HPA/LNA health, interference environment and local environmental risk. Emergency architecture should avoid dependence on a single high-throughput but weather-sensitive band. A robust design combines low-rate robust paths with high-capacity paths.

Band / bearer	Emergency value	Risks	Recommended use
L-band	Robust, mobile, weather-resilient	Low data rate and scarce spectrum	Life-safety voice, messaging, tracking, basic command
S-band	Moderate robustness	Limited capacity	TT&C, selected emergency links
X-band	Government/science missions	Restricted access, specialized terminals	Protected mission and EO downlink contexts
Ku-band	Good capacity and terminal ecosystem	Rain fade, congestion	VSAT, mobile backhaul, NGO and response teams
Ka-band	High throughput	Strong rain attenuation, precise pointing	High-capacity restoration with site diversity
Optical	Very high throughput, low intercept risk	Weather/cloud sensitivity and pointing complexity	Trunking between resilient sites, future high-assurance links
Terrestrial fibre/microwave	High capacity and low latency	Physical damage, power dependency	Primary/alternate when intact
D2D/NTN	Reach ordinary devices	Capacity and standardization limits	Warning, SMS, priority low-rate services

5.2 Link, network and transport layer

At the link layer, IFECS should support both space-specific protocols and terrestrial IP integration. CCSDS TM/TC/AOS, SLE/CSTS, DVB-S2X/RCS2, proprietary commercial waveforms, 5G NTN and IP/MPLS overlays may all coexist. The emergency architecture should not force a single waveform. Instead, it should wrap heterogeneous waveforms behind service adapters and expose standard service descriptors to brokers.

For intermittent or damaged connectivity, DTN is essential. BPv7 allows information to be packaged into bundles that can be stored and forwarded when connectivity becomes available. This is useful when LEO contact windows, damaged terrestrial backhaul, mobile gateway movement or cyber quarantine prevent continuous end-to-end IP connectivity.

5.3 Ground-station service descriptor

The Emergency Ground Service Descriptor, or EGSD, is one of the central technical proposals. It is a signed machine-readable object published by each station or operator through its national node. EGSD must be detailed enough to allow compatibility and routing decisions but not so detailed that it exposes classified, commercially sensitive or cyber-sensitive information.

EGSD field	Example content	Security treatment
Station identity	Operator, country, station class, emergency contact	Signed, public or restricted
Coordinates / coverage	Exact or generalized site and visibility mask	Exact data may be restricted
RF capabilities	Bands, EIRP class, G/T class, antenna size class	Classified abstraction for sensitive sites
Waveforms / protocols	CCSDS, SLE/CSTS, DVB-S2X, 5G NTN, IP, DTN	Restricted when needed
Service types	TT&C relay, EO downlink, IP backhaul, CAP alert broadcast	Shared with brokers
Availability	Nominal, degraded, emergency-only, offline	Real-time restricted metadata
Cyber posture	Trusted, suspect, quarantined, clean-core only	Restricted, signed, auditable
Legal constraints	Domestic only, regional, humanitarian, classified, operator approval required	Policy-controlled
Priority classes accepted	Life safety, government, hospital, public alert, humanitarian	Shared with brokers
Contact method	API endpoint, emergency desk, out-of-band number	Restricted

6. Ground-to-Ground Interconnection Between Stations

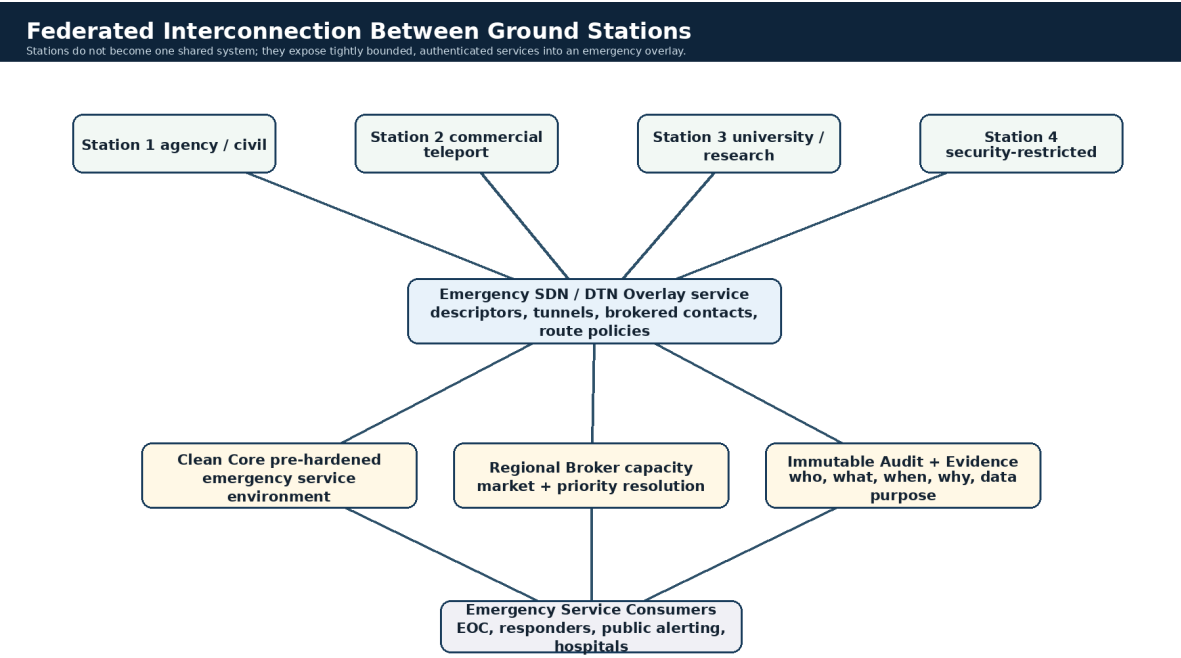


Figure 4. Federated interconnection between ground stations through an emergency overlay.

Ground stations should not be connected by flat network peering. A flat interconnection model would expose internal station systems to cyber compromise, configuration errors and unauthorized access. Instead, stations should connect through segmented emergency gateways using mutually authenticated tunnels, policy-controlled service exposure and independent logging. The goal is not to make every station operate every satellite; the goal is to make station services discoverable, requestable, auditable and routable when compatibility and authorization exist.

6.1 Recommended interconnection model

Layer	Implementation option	Purpose
Physical connectivity	Fibre, microwave, satellite trunk, leased lines, secure internet VPN	Provide diverse paths between station adapters and brokers
Transport	IP/MPLS, SD-WAN, QUIC/TLS, DTN overlay	Support both real-time and disrupted environments
Service gateway	API gateway, message broker, service mesh, SLE/CSTS gateway	Expose bounded station services
Security	mTLS, HSM-backed keys, hardware roots of trust, short-lived tokens	Authenticate identities and prevent credential reuse
Policy	ABAC/RBAC, sovereign approval, purpose limitation	Control who can request what service and why
Operations	NOC/SOC integration, alerting, SIEM, immutable logs	Maintain monitoring, forensics and accountability

6.2 Emergency SDN and DTN overlay

A dual overlay is recommended. The SDN/SD-WAN layer supports real-time IP traffic where connectivity exists. The DTN layer supports delayed, intermittent or quarantined connectivity. Emergency routing policies should classify flows into real-time, delay-tolerant and store-and-forward categories.

Traffic type	Recommended path	Latency tolerance	Examples
Life-safety voice	Real-time IP/SATCOM/public safety radio	Seconds	EOC coordination, ambulance dispatch
CAP public alert	Broadcast/SMS/D2D/satellite	Seconds to minutes	Evacuation instruction, tsunami warning
EO raw data	High-capacity link or DTN	Minutes to hours	SAR flood imagery, optical damage images
Maps and analytics	IP/DTN mixed	Minutes	Flood extent, road closures, shelter maps
Logs and evidence	DTN with integrity protection	Minutes to days	Audit bundles, forensic snapshots
Administrative traffic	Best effort	Hours	Routine reporting

PART III

FAILOVER, CYBERSECURITY & DATA ASSURANCE

Bounded autonomy, PACE routing, clean-core operation, sovereign database federation and human control.



7. Autonomous Failover Design

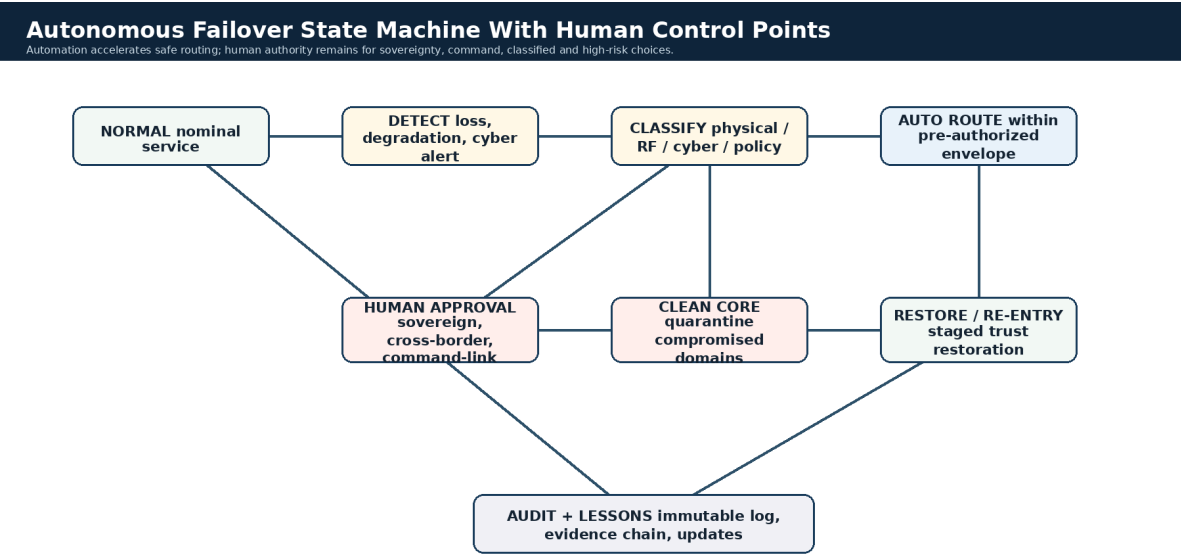


Figure 5. Failover state machine with human control points.

Autonomous failover is necessary because the first minutes of a catastrophe can determine whether warnings are delivered and responders remain coordinated. However, autonomy must be bounded. The architecture therefore defines failover envelopes. Inside an envelope, systems may reroute traffic automatically. Outside it, the system must pause for human or sovereign authorization.

7.1 PACE architecture

PACE level	Example path	Decision mode	Use case
Primary	Domestic terrestrial fibre + operational national gateway	Automatic	Normal emergency operations
Alternate	Domestic satellite gateway or commercial teleport	Automatic if pre-authorized	Fibre cut, tower failure
Contingency	Regional brokered ground station in neighbouring country	Human or sovereign approval unless pre-cleared	National gateway unavailable
Emergency	D2D, L-band, radio, airborne relay, clean-core-only service	Emergency authority approval; may be automated for public alerting	Complete infrastructure collapse or cyber quarantine

7.2 Failover triggers

Trigger category	Examples	Automated action	Human decision point
Physical failure	Power loss, flooded station, antenna fault, fibre cut	Switch to alternate station/path; start restoration ticket	Use foreign station or classified asset
Performance degradation	Packet loss, latency, congestion, rain fade	Adjust coding, shift traffic class, reroute noncritical flows	Drop lower-priority services
Cyber compromise	Credential anomaly, malware, destructive command attempt	Quarantine, revoke trust, shift to clean core	Re-entry and attribution-sensitive actions

Trigger category	Examples	Automated action	Human decision point
RF interference	Jamming, spoofing, adjacent-satellite interference	Shift band/site/orbit, activate interference monitoring	Escalate to regulator/security authority
Legal/policy conflict	Capacity requested across border or for security service	Hold request and route to approval workflow	Authorize sovereign exception

7.3 Safe autonomy rules

- Autonomy may reroute data traffic but must not independently change spacecraft command authority across sovereign boundaries.
- Autonomy may prioritize life-safety traffic according to pre-approved policies but must log all de-prioritization of other traffic.
- Autonomy may quarantine a compromised node but must provide an out-of-band restoration path for emergency override by authorized officials.
- Autonomy may generate recommendations for spectrum or cross-border use but must not transmit in unauthorized bands without legal emergency authority.
- AI models must be advisory for high-consequence decisions, with deterministic rule engines used for safety-critical authorization gates.

8. Cybersecurity and Cyberattack Contingency

Cyberattack is not an exceptional edge case; it is a central design driver. Satellite communications systems, ground networks and emergency databases are attractive targets during disasters and security crises because they influence public warning, command and control, logistics, media narratives and critical infrastructure restoration. The contingency architecture must assume compromise and continue minimum life-safety services under degraded trust.

8.1 Threat model

Threat	Possible effect	IFECS control
Credential theft	Unauthorized service requests, route changes, data access	Short-lived credentials, HSM-backed keys, phishing-resistant MFA, behavioural monitoring
Ransomware	Loss of station/NOC systems	Offline backups, clean-core operations, segmented station adapters
Destructive malware	Loss of modems, routers, terminals, user devices	Golden images, replacement kits, staged re-entry, device attestation
Supply-chain compromise	Trusted software/hardware becomes attack vector	SBOM, signed builds, vendor diversity, red-team testing
DDoS	Control/API saturation	Rate limiting, scrubbing, degraded offline workflows, DTN queues
GNSS spoofing	Antenna pointing/timing error, wrong geolocation	Multi-source timing, inertial backup, authenticated GNSS when available
RF jamming	Loss of link availability	Band/orbit/site diversity, interference geolocation, adaptive coding
Insider threat	Improper approvals or data exposure	Dual-control, least privilege, immutable audit, anomaly detection
Database exfiltration	Exposure of shelters, critical infrastructure or personal data	Purpose-bound query tokens, redaction, encryption, data minimization

8.2 Clean-core operating mode

The clean core is a pre-hardened, isolated operating environment used when normal networks are suspect. It contains only minimum emergency services: identity verification, public alert routing, station service descriptors, priority routing, selected situational-awareness feeds, emergency maps and immutable logging. It must be tested regularly, operated from separate infrastructure and reachable through independent out-of-band communications.

8.3 Trust revocation and staged re-entry

When a station, operator, national node or software component becomes suspect, IFEGS must support immediate trust revocation. Revocation should not mean complete operational silence. Instead, the system should offer graded trust states: trusted, restricted, monitor-only, receive-only, clean-core-only, quarantined and re-entry candidate. Re-entry requires forensic review, reimaging or attestation, key rotation, policy approval and heightened monitoring.

9. Secure Database and Information Exchange Architecture

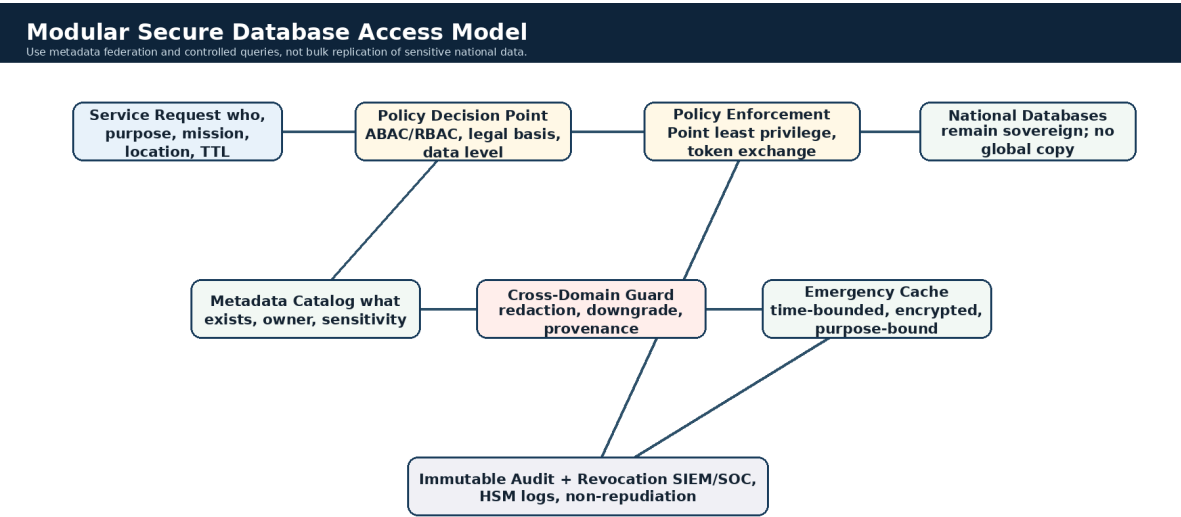


Figure 6. Modular database access architecture with sovereign control.

Emergency communications are inseparable from data. A functioning link without trusted data may not save lives; trusted data without communications may never reach responders. However, centralizing all disaster, telecom, infrastructure and population databases would create severe security and sovereignty risks. IFEGS therefore uses a modular data federation model.

9.1 Data categories

Data class	Examples	Default access rule
Public hazard data	Weather warnings, flood alerts, wildfire perimeters	Open or broadly shareable
Operational disaster data	Road closures, shelter locations, hospital status	Restricted to authorized responders
Telecom infrastructure data	Tower status, gateway routes, backhaul maps	Restricted; may be sensitive for security and commercial reasons

Data class	Examples	Default access rule
Ground-station data	Exact capabilities, locations, cyber state	Restricted, classified abstraction allowed
Personal data	Evacuee lists, medical needs, family reunification	Strict purpose limitation and minimization
Security/classified data	Military networks, protected assets, sensitive ISR	Separate domain; no automatic release
Cyber forensic data	Indicators, logs, malware details, compromised accounts	Need-to-know, evidentiary handling

9.2 Access control model

Access should be controlled through attribute-based and role-based access with purpose-bound claims. Every request should answer: who is asking, on behalf of which authority, for what mission, for which geographic area, for how long, at what sensitivity level, under which legal basis and with what retention obligation. Emergency does not eliminate data protection; it changes the legal basis and urgency under controlled rules.

9.3 Database federation pattern

- Do not copy sensitive national databases into a global repository.
- Publish a metadata catalogue indicating that a data product exists, its owner, sensitivity, update rate and access procedure.
- Use policy decision points and enforcement points to grant minimum necessary access.
- Use cross-domain guards to redact, aggregate or downgrade data before sharing across domains.
- Use time-limited encrypted caches only for operational continuity, with expiry and deletion proof.
- Require provenance metadata so responders know source, timestamp, confidence and constraints.

10. Human Factors, Human Intervention and Error Control

Major failures in emergency communications are often caused not by absent technology but by human overload, unclear authority, wrong configuration, misunderstood procedures, language barriers or fatigue. The architecture therefore includes explicit human-factor controls.

Human risk	Example	Mitigation
Configuration error	Wrong frequency, wrong beam, wrong modem profile	Pre-validated profiles, digital checklists, simulation drills
Wrong prioritization	Noncritical traffic consumes emergency bandwidth	Predefined priority classes and automatic enforcement
Phishing/social engineering	Attacker impersonates emergency authority	Verified contact directory, voice callback, cryptographic request signing
Operator fatigue	Mistakes after long shifts	Shift limits, dual control, automation for routine tasks
Ambiguous authority	Multiple actors issue conflicting requests	Incident command hierarchy and regional arbitration rules
Language mismatch	Alerts not understood by affected population	CAP multilingual templates and local validation
Over-trust in AI	Operator accepts unsafe recommendation	Explainable recommendations and mandatory human approval for high-risk actions

10.1 Human-in-the-loop thresholds

Action	Automation allowed?	Required approval
Shift noncritical IP traffic to alternate domestic gateway	Yes	Logged operator notification
Activate D2D public warning template	Yes if pre-approved	Civil protection authority validation for message content
Use foreign ground station for domestic EO downlink	Conditional	National node and regional broker approval
Route spacecraft command through foreign station	Normally no	Mission owner plus sovereign authority plus dual-person control
Release personal evacuation database to external NGO	No automatic release	Data controller and emergency authority approval
Quarantine compromised node	Yes	SOC confirmation and incident commander notification
Reintegrate compromised node	No	Forensic, security and operational approval

PART IV

CRISIS SCENARIOS, GOVERNANCE & LAW

Operational scenarios, strategic architecture, governance, regulation and emerging capabilities.



11. Concrete Crisis Scenarios

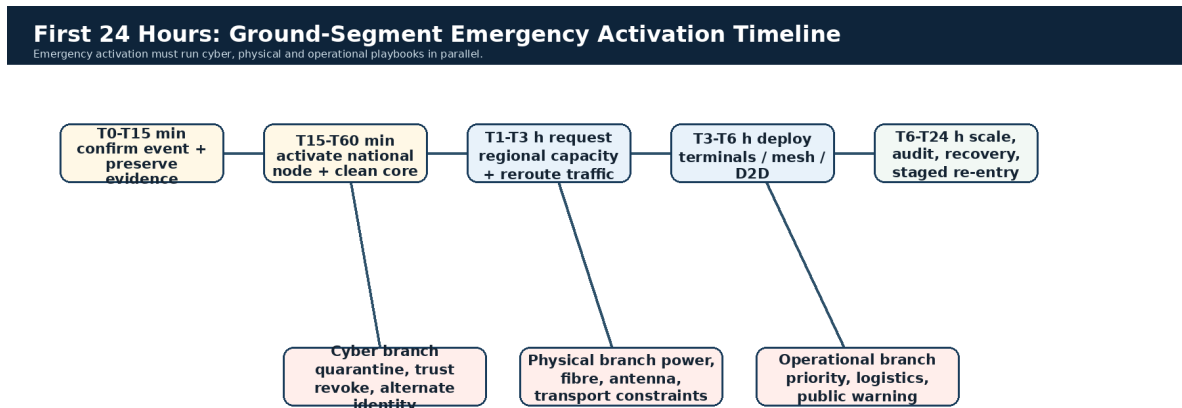


Figure 7. First 24-hour activation timeline across physical, cyber and operational branches.

11.1 Global climate catastrophe: synchronized floods across multiple river basins

Scenario: several regions experience severe floods during an extreme rainfall season. Terrestrial mobile networks are overloaded; rural fibre is damaged; some ground gateways remain operational but are congested. The goal is to preserve public warning, hospital connectivity, flood mapping and cross-border logistics.

- T0-T15 minutes: meteorological and hydrological systems issue warnings using CAP templates. National nodes validate public warning messages and deliver through cell broadcast, radio, apps and satellite D2D where terrestrial coverage is weak.
- T15-T60 minutes: national ground-segment registries mark flooded stations, power-constrained sites and available commercial satellite capacity. Clean-core systems are placed on standby.
- T1-T3 hours: regional broker reallocates noncritical EO downlinks to unaffected stations, prioritizes SAR flood imagery and assigns LEO/MEO backhaul to hospitals and EOCs.
- T3-T12 hours: portable terminals and mesh nodes are moved to shelters and medical triage points. DTN is used for non-real-time map products and logistics data.
- T12-T24 hours: data catalogue is updated with flood extent, road closures, shelter capacity and power restoration status. Priority rules are revised based on life-safety demand.

11.2 National earthquake plus cyberattack on satellite/telecom infrastructure

Scenario: a major earthquake damages fibre routes and cellular towers. At the same time, operators detect credential compromise and destructive malware against satellite gateway management systems. The objective is to restore life-safety communications without spreading the compromise.

- Immediate: affected gateways move to restricted status; compromised credentials are revoked; the clean core is activated.
- Routing: life-safety traffic is shifted to pre-approved L-band, GEO/MEO backup and unaffected regional LEO gateways. High-bandwidth but noncritical traffic is delayed or moved to DTN queues.
- Command safety: spacecraft command links are frozen to known-good paths unless mission owner and sovereign authority approve an alternate route.

- Data safety: operational maps are shared through cross-domain guards; exact critical-infrastructure data remains restricted.
- Recovery: compromised systems re-enter only after forensic review, reimaging, key rotation and staged monitoring.

11.3 Regional security crisis: jamming, spoofing and sensitive civil/security boundary

Scenario: a border-region disaster occurs during heightened security tensions. RF interference affects satellite links; GNSS spoofing is detected; foreign rescue teams request access to communications and situational data. The objective is to keep humanitarian communications functioning while protecting national security and avoiding uncontrolled escalation.

- RF response: affected links shift to alternate bands, beams, sites or orbits; interference data is logged for regulatory/security channels.
- GNSS response: timing sources switch to multi-source time references; location products are marked with confidence metadata.
- Data boundary: humanitarian layers are separated from classified/security layers; responders receive route, shelter and medical logistics data without sensitive security overlays.
- Legal process: regional broker handles capacity requests but national node approves any foreign station use or protected service routing.
- Public messaging: CAP alerts are validated by civil authority to avoid misinformation and panic.

11.4 Small island cyclone: complete terrestrial backhaul collapse

Scenario: a cyclone disables submarine cable landing points, cellular towers, grid power and airport operations. Local emergency management requires connectivity before major equipment can arrive. The objective is minimum communications survival within the first hours.

- Immediate: D2D/SMS alerting and radio are used for public warning; satellite phones support initial command links.
- First hours: pre-positioned portable terminals are activated at EOC, hospital, port and shelter sites; solar/battery kits extend autonomy.
- Regional support: regional broker assigns spare satellite capacity and identifies external gateways not affected by the cyclone.
- Data: shelter status and medical requests are synchronized through DTN when continuous IP service is unavailable.
- Recovery: mobile base stations with satellite backhaul re-establish local cellular islands.

11.5 Multi-region public health/logistics crisis

Scenario: a disease outbreak or mass displacement crisis requires secure data exchange among health authorities, border agencies, humanitarian actors and telecom operators. The communications network itself remains partially functional but data access and privacy risks dominate.

- Identity: responders authenticate through emergency federation but access only mission-specific data.
- Data minimization: personal health data is aggregated or pseudonymized where possible.
- Communications: satellite links provide connectivity to temporary clinics and remote camps.
- Audit: every personal-data query is logged with purpose, authority, geographic scope and retention time.
- Legal: information sharing follows pre-agreed emergency data-processing clauses.

12. Strategic Architecture and Governance

IFEGS is a strategic architecture as much as a technical system. It touches sovereignty, critical infrastructure protection, commercial service obligations, military-civil boundaries, humanitarian access, space security, spectrum management and data protection. Its governance must therefore be layered.

Level	Primary responsibilities	Participants
National	Asset registry, sovereign approvals, spectrum, public warning, domestic legal basis	Telecom regulator, space agency, civil protection, defence/security, operators
Regional	Capacity brokerage, cross-border escalation, regional exercises, mutual assistance	Regional organizations, neighbouring states, satellite operators, humanitarian bodies

Level	Primary responsibilities	Participants
Global	Standards, trust federation, emergency metadata exchange, legal model clauses, global exercises	ITU, UN agencies, space agencies, standards bodies, operators
Commercial	Service availability, emergency SLAs, cyber posture, capacity reporting	Satellite operators, ground station networks, MNOs, cloud/edge providers
Humanitarian	Needs assessment, field terminals, last-mile operations, community feedback	UN, NGOs, Red Cross/Red Crescent, local civil society

12.1 Civil-security separation

The architecture must permit cooperation between civil protection and security actors without transforming humanitarian connectivity into an uncontrolled security system. Recommended separation mechanisms include distinct service classes, clear authority chains, labelled data domains, mission-specific tokens, cross-domain guards and audit rules that document whether traffic is humanitarian, public-safety, government continuity, critical infrastructure or security-related.

12.2 Commercial participation

Commercial satellite and ground-station operators are essential because they own much of the deployable capacity. Their participation requires contractual clarity: emergency priority classes, compensation models, liability limits, pre-agreed technical interfaces, lawful access constraints, cyber incident notification, service availability targets and rules for public communication. Emergency capacity should be a standing service product, not an improvised goodwill arrangement.

12.3 Exercises and certification

No architecture should be trusted without exercises. Each participating station, operator and national node should undergo certification including tabletop exercises, live failover tests, cyber red-team tests, database access drills, public warning simulations and regional mass-casualty scenarios. Certification should expire and require renewal.

13. Legal and Regulatory Framework

The legal framework must reconcile urgency with sovereignty. Disaster telecommunications often require rapid importation of equipment, temporary spectrum use, cross-border support, foreign personnel, data sharing and commercial service activation. The Tampere Convention already provides a foundation for reducing regulatory barriers to disaster telecommunications, while preserving the affected state's authority. ITU Resolution 647 provides spectrum management guidance for emergency and disaster relief radiocommunications. The Outer Space Treaty remains relevant for state responsibility and international cooperation in space activities. Cybersecurity and data protection frameworks add further obligations.

Legal instrument / domain	Relevance to IFECS	Gap or action needed
Tampere Convention	Facilitates disaster telecommunications assistance and regulatory barrier reduction	Operationalize model clauses for ground-station federation and satellite capacity brokerage
ITU Radio Regulations / Resolution 647	Emergency/disaster radiocommunication spectrum management	Pre-register emergency frequency/band procedures and temporary authorizations
Outer Space Treaty Articles VI-IX	State responsibility, authorization, supervision, due regard and harmful interference	Clarify cross-support obligations and emergency service routes involving private operators
NIS2 and national cybersecurity laws	Critical infrastructure cybersecurity, incident reporting, cross-border coordination	Map satellite ground stations and emergency brokers into critical entity obligations
Data protection laws / GDPR-type frameworks	Personal data, health data, location and evacuation data	Predefine emergency lawful bases, minimization and retention rules

Legal instrument / domain	Relevance to IFECS	Gap or action needed
International humanitarian and disaster law	Access, assistance, consent and neutrality	Ensure humanitarian traffic is protected and not misused
Commercial contracts and SLAs	Emergency priority, liability, compensation, service restoration	Develop standard emergency clauses across operators
Export control / sanctions	Equipment, encryption, satellite terminals and software movement	Pre-clear humanitarian exceptions and emergency licensing paths
National security law	Classified networks and protected assets	Define civil/security interfaces and cross-domain release procedures

13.1 Proposed model legal clauses

- Emergency Service Exposure Clause: participating stations agree to expose defined emergency services through signed EGSD objects, subject to national approval.
- Emergency Priority Clause: life-safety communications may receive pre-agreed priority over noncritical traffic during declared emergencies.
- Sovereign Approval Clause: cross-border use of ground infrastructure requires either pre-cleared classes or rapid national node approval.
- Cyber Trust Clause: parties must support emergency credential revocation, compromise notification and staged re-entry procedures.
- Data Minimization Clause: participating parties exchange only minimum necessary data for the declared emergency purpose.
- Liability and Compensation Clause: operators receive protection and compensation for good-faith emergency support within agreed rules.
- Audit and After-Action Clause: all emergency actions are logged and reviewed without exposing protected/classified details beyond the agreed scope.

14. Emerging Technologies and Planned Capabilities

IFECS should be designed to absorb emerging systems rather than depend on them from day one. The most relevant trajectory is convergence: satellite networks, terrestrial mobile systems, cloud/edge infrastructure and public-safety communications are moving toward tighter integration.

Emerging capability	Expected contribution	Integration requirement
5G/6G NTN	Satellite access integrated with mobile standards	Priority services, emergency roaming, handset support
Direct-to-device satellite	Reach ordinary smartphones beyond terrestrial coverage	Capacity governance, public warning profiles, regulatory authorization
Multi-orbit secure connectivity systems	Sovereign/government resilient broadband	Interfaces to regional brokers and public-safety services
Optical inter-satellite and ground links	High-capacity, lower intercept, resilient routing	Weather diversity and fallback RF paths
HAPS/UAV relay	Temporary local 4G/5G/Wi-Fi coverage with satellite backhaul	Aviation permissions, spectrum and rapid deployment kits
AI NOC/SOC assistants	Anomaly detection, contact scheduling, routing recommendations	Explainability, audit, safe-mode rules
Post-quantum cryptography	Future protection against quantum-enabled decryption	Crypto agility and migration plan
Digital twins	Training and pre-event resilience simulation	Data accuracy and continuous update
Space-based cloud/edge processing	On-orbit prioritization and pre-processing	Trust, data sovereignty and payload constraints

PART V

STANDARDS, ROADMAP & TECHNICAL ANNEXES

Gap closure, proposed standards family, implementation roadmap, activation checklist and engineering annexes.



15. Missing Gaps

Gap	Why it matters	Proposed closure
No global emergency ground-service descriptor	Stations cannot advertise compatible emergency services safely and consistently	Standardize EGSD
Weak cross-operator emergency roaming	Capacity exists but cannot be dynamically allocated	Create regional capacity brokers and emergency SLAs
Insufficient legal pre-clearance	Permissions are negotiated during crisis	Model clauses and pre-approved service classes
Gateway and ground-station single points of failure	Space segment survives but service fails on the ground	Site diversity, clean core, alternate gateways, DTN
Cyber trust fragmentation	A compromised node may contaminate others or be isolated too broadly	Federated trust states and revocation protocols
Data sovereignty tension	Useful data cannot be shared or is over-shared unsafely	Metadata federation, cross-domain guards, purpose-bound access
Human procedure inconsistency	Different agencies use incompatible workflows	Joint exercises, digital runbooks, certification
Limited last-mile reach	Remote and vulnerable communities remain disconnected	D2D, L-band, mesh, portable terminals, community radio
No unified priority framework	Bandwidth is allocated inconsistently	Life-safety priority classes and traffic labels
Poor interoperability testing	Interfaces are assumed but not exercised	Annual live regional and inter-regional failover drills

16. Recommended Standards Family

A dedicated IFECS standards family should be proposed to existing standards bodies rather than launched as an isolated proprietary architecture. The family could be developed through a combination of ITU, CCSDS, OASIS, 3GPP liaison, ISO/IEC cybersecurity working groups and regional telecommunications bodies.

Proposed standard	Content
IFECS-001: Emergency Ground Service Descriptor	Machine-readable station/service capability, sensitivity, legal status and cyber trust metadata
IFECS-002: Emergency Capacity Brokerage API	Requests, offers, priorities, allocations, denial reasons and audit objects
IFECS-003: Federated Trust and Identity Profile	PKI, mTLS, HSM, token lifetime, revocation, emergency roles
IFECS-004: PACE Failover Safety Profile	Allowed autonomous actions, thresholds, fallback paths and human authorization gates
IFECS-005: Secure Disaster Data Exchange	Metadata catalogue, purpose-bound queries, provenance, retention and redaction
IFECS-006: Clean-Core Operations	Minimum emergency services, isolation, backups, re-entry and monitoring
IFECS-007: Cyber Incident Federation	Trust states, compromise reports, indicators, evidence handling and escalation
IFECS-008: Emergency Priority and QoS Labels	Life-safety classes, public warning, hospital, infrastructure, humanitarian and best-effort traffic
IFECS-009: Legal and Commercial Emergency Clauses	Model agreements for operators, states and humanitarian actors
IFECS-010: Exercise and Certification Scheme	Test procedures, red-team requirements, renewal and maturity levels

17. Implementation Roadmap

Phase	Timeline	Main deliverables
Phase 0: concept alignment	0-6 months	Institutional sponsorship, stakeholder map, draft EGSD, legal gap analysis
Phase 1: national pilots	6-18 months	Two to five national nodes, station registries, clean-core prototype, tabletop exercises
Phase 2: regional broker pilot	18-30 months	Regional broker, capacity APIs, live domestic/regional failover test, emergency SLA templates
Phase 3: inter-regional federation	30-48 months	Global metadata exchange, trust federation, multi-region cyber/flood exercise
Phase 4: advanced autonomy	48-72 months	AI-assisted NOC/SOC, 5G NTN/D2D integration, PQC migration, digital twins
Phase 5: standing operational capability	72+ months	Certification programme, annual exercises, permanent emergency capacity markets

17.1 Minimum national readiness baseline

- National ground-station and satellite gateway inventory with emergency capability classification.
- Designated national sovereign node and 24/7 emergency communications contact.
- At least one clean-core environment and one out-of-band communications path.
- Pre-approved PACE paths for public warning, EOC connectivity, hospital connectivity and EO data exchange.
- Legal procedure for temporary spectrum, terminal import and cross-border support.
- Cyber incident playbook including revocation, quarantine and re-entry.
- Annual exercise involving civil protection, telecom regulator, operators and at least one external partner.

18. 24-Hour Activation Checklist

Time window	Action
0-15 minutes	Confirm incident class; preserve logs; activate incident command; validate public warning authority
15-30 minutes	Check station/gateway health; publish degraded status; activate clean-core standby
30-60 minutes	Apply priority classes; shift traffic to primary/alternate paths; revoke suspect credentials
1-3 hours	Request regional capacity if national paths are degraded; activate portable terminals and mesh plan
3-6 hours	Synchronize hazard maps, telecom outage data and shelter/hospital status through secure catalogues
6-12 hours	Scale capacity; deploy mobile gateways; isolate compromised domains; update public warnings
12-24 hours	Stabilize service, document exceptions, begin staged restoration and prepare after-action evidence

19. Technical Annex A: Link Engineering Considerations

Emergency planners often underestimate link engineering. A contingency plan must precompute link budgets and availability assumptions for each station/service pair. The following parameters should be recorded in the EGSD or a restricted engineering annex.

Parameter	Why it matters
Antenna diameter and gain class	Determines achievable data rates, link margin and satellite compatibility
G/T and system noise temperature	Impacts uplink/downlink performance and weather resilience
EIRP / HPA class	Limits uplink performance and regulatory exposure
Pointing and tracking accuracy	Critical for high-frequency bands and LEO tracking
Polarization support	A mismatch can cause severe performance degradation
Modulation and coding profiles	Determines interoperability and adaptive response to fading
Rain zone and local climate	Critical for Ka/Q/V availability planning
Power autonomy	Determines survivability after grid failure
Backhaul alternatives	Fibre, microwave, satellite trunk and DTN fallback
Time and frequency reference	GNSS dependency and backup timing options
Cyber boundary	Which systems are exposed, isolated or clean-core compatible

20. Technical Annex B: Sample EGSD Object

A simplified conceptual EGSD structure is shown below. Actual implementation should use a formal schema such as JSON Schema with digital signatures, versioning and sensitivity marking.

```
{
  "egsd_version": "0.9-draft",
  "station_id": "IFEGS-NAT-A-GS-014",
  "operator": "National Space Agency / Commercial Partner",
  "country": "ExampleState",
  "services": ["eo_downlink", "ip_backhaul", "dtn_forwarding", "cap_broadcast"],
  "rf_capabilities": {
    "bands": ["S", "X", "Ku", "Ka"],
    "availability_class": "99.5-emergency",
    "weather_risk": "ka_rain_fade_high"
  },
  "protocols": ["CCSDS_TM_TC", "SLE", "IPsec", "DTN_BPv7"],
  "legal_scope": ["domestic", "regional_humanitarian_preapproved"],
  "cyber_trust_state": "trusted",
  "priority_classes": ["life_safety", "public_warning", "hospital", "eo_mapping"],
  "data_sensitivity": "restricted_metadata",
  "approval_required_for": ["telecommand", "foreign_security_traffic"],
  "contact_endpoint": "https://national-node.example/ifeqs/service-request",
  "signature": "detached-signature-reference"
}
```

21. Technical Annex C: Recommended Emergency Priority Classes

Priority	Traffic class	Examples	Preemption rights
P0	Distress and life safety	SOS, search and rescue, medical evacuation	May preempt all lower classes

Priority	Traffic class	Examples	Preemption rights
P1	Public warning	Tsunami/flood/earthquake alerts, evacuation orders	May preempt P2-P5
P2	Emergency command	EOC, police/fire/medical coordination	May preempt P3-P5
P3	Critical infrastructure	Power, water, telecom restoration	May preempt P4-P5
P4	Humanitarian operations	Shelters, logistics, NGOs, family reunification	May preempt P5
P5	General public connectivity	Best-effort internet access	No preemption rights

22. Conclusion

The most important conclusion is that the global ground segment cannot be made resilient simply by adding more antennas or more satellites. Resilience requires federation: technical federation, trust federation, legal federation and operational federation. The recommended architecture preserves national sovereignty, protects sensitive databases, enables cross-border emergency capacity, supports autonomous failover within safe limits and treats cyberattack as a core operating condition. The result is a practical path toward a global emergency ground-segment capability that can be implemented region by region and institution by institution without waiting for a single global authority or a single new constellation.

IFECS should be advanced as a standards-led and exercise-led initiative. The first practical step is not to build a global platform, but to define the emergency ground service descriptor, create national station registries, establish regional capacity-broker pilots and test clean-core failover in realistic cyber-physical disaster scenarios.

References and Source Base

1. CCSDS. Guidelines for the Specification of Cross Support Transfer Services, CCSDS 921.2-M-1, March 2019.
2. CCSDS. Space Link Extension and Cross Support Transfer Services publications and working group material.
3. IETF RFC 9171. Bundle Protocol Version 7.
4. IETF RFC 9172. Bundle Protocol Security Protocol Specification.
5. NASA. Delay/Disruption Tolerant Networking overview and technical material.
6. OASIS. Common Alerting Protocol Version 1.2, approved 1 July 2010.
7. ITU. Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations.
8. ITU. Resolution 647 (WRC-07), Spectrum management guidelines for emergency and disaster relief radiocommunication.
9. ITU. Emergency telecommunications, Early Warnings for All connectivity mapping and Disaster Connectivity Map material.
10. 3GPP. Non-Terrestrial Networks overview and Release 17/18 NTN work items.
11. European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2).
12. European Commission / ESA. IRIS² secure connectivity programme public information and factsheets.
13. WMO / UNDRR. Global Status of Multi-Hazard Early Warning Systems 2025.
14. Outer Space Treaty, 1967, Articles VI, VII, VIII and IX.
15. Relevant public reporting and official communications on the 2022 KA-SAT cyberattack and satellite communications resilience lessons.

PART VI

DETAILED ENGINEERING & INSTITUTIONALIZATION

Detailed signal-chain engineering, inter-station connectivity, multi-orbit integration, validation, procurement, financing and policy.

23. Detailed Communications Engineering Between Satellite and Ground Station

This section expands the communications engineering basis of the contingency plan. A satellite-ground link is not a binary connection; it is a chain of physical, protocol, operational and security conditions. Emergency failover must therefore check link feasibility before allocating an alternate station. A broker that allocates a contact without validating these conditions can create false resilience: the route exists on paper but fails operationally.

23.1 End-to-end signal path

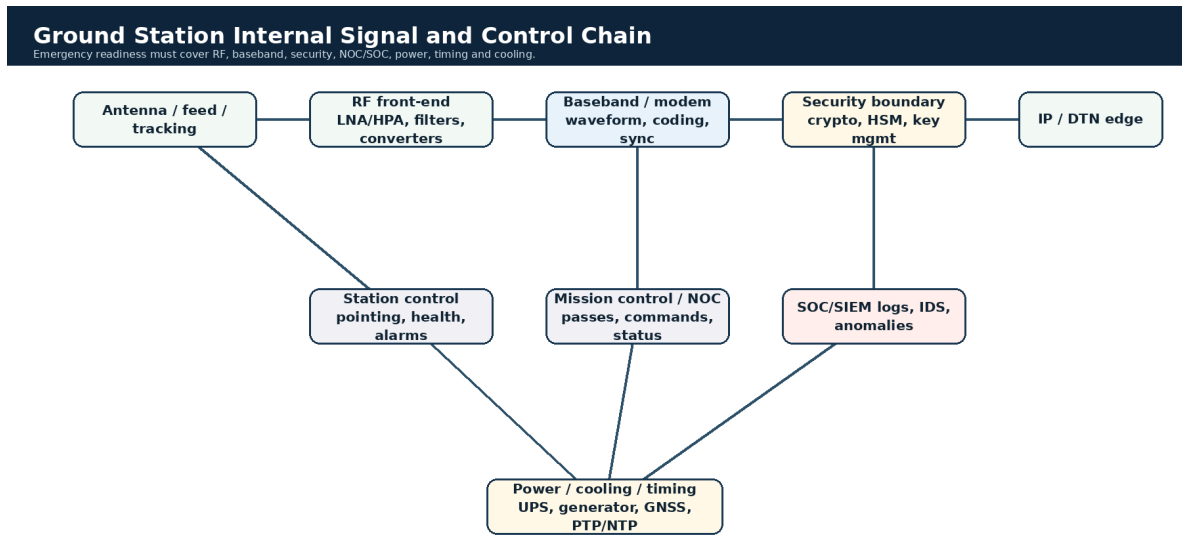


Figure 8. Ground station internal signal and control chain.

The signal path begins with antenna pointing and polarization alignment, proceeds through low-noise amplification or high-power amplification, frequency conversion, filtering, baseband demodulation or modulation, synchronization, coding, framing, decryption/encryption, packetization and routing. Every element can be a failover constraint. For example, a station may support Ka-band but not the exact waveform, may have the right antenna but not the right crypto module, or may support the downlink but not authorized telecommand uplink.

23.2 Link budget parameters to pre-compute

Parameter	Definition	Emergency relevance
EIRP	Effective isotropic radiated power from satellite or ground transmitter	Determines uplink/downlink margin; may be limited by licence or amplifier class
G/T	Antenna gain-to-noise-temperature ratio	Determines receive sensitivity and data-rate feasibility
C/N0	Carrier-to-noise density ratio	Primary indicator for link performance and adaptive coding decisions
Eb/N0	Energy per bit to noise density	Used to determine modulation/coding feasibility and BER margin
BER / PER	Bit or packet error rate	Directly impacts usable throughput and retransmission burden

Parameter	Definition	Emergency relevance
Availability target	Percentage of time link meets minimum service level	Disaster services require explicit degraded-service classes
Rain fade margin	Link margin reserved for precipitation attenuation	Critical for Ku/Ka/Q/V bands in tropical and cyclone conditions
Pointing loss	Loss caused by antenna tracking error	Important for LEO and high-frequency links
Interference margin	Reserved margin for unintentional or hostile interference	Critical in hybrid/security crises
Regulatory PFD/EPFD limits	Power flux-density constraints	Prevents harmful interference and maintains legal compliance

23.3 Service classes for satellite-ground links

Service class	Performance objective	Suitable links	Notes
Class A: distress and control	High availability, low bandwidth, highest priority	L-band, protected GEO/MEO, public-safety radio, D2D emergency	Must survive extreme degradation; no video or routine data
Class B: emergency command	Low latency when possible; reliable voice/data	LEO/MEO/GEO, terrestrial if intact	Requires QoS and preemption of lower classes
Class C: operational data	Moderate bandwidth, integrity and provenance	LEO/MEO/GEO/IP/DTN	Maps, logistics, responder positions and hospital status
Class D: EO and analytics	High bandwidth; delay-tolerant	LEO/MEO/ground-station downlinks/DTN	Can be queued and forwarded through unaffected stations
Class E: public connectivity	Best effort after critical services	LEO/GEO Wi-Fi hotspots, temporary cellular	Must not consume life-safety capacity

23.4 Contact-window planning

LEO and some MEO services require attention to contact windows. Even when user service appears continuous through a constellation, the underlying gateway and crosslink paths remain constrained by visibility, gateway availability, inter-satellite-link topology, regulatory landing rights and network policy. For EO downlink and TT&C cross-support, contact scheduling remains explicit. The emergency broker should therefore solve a constrained scheduling problem.

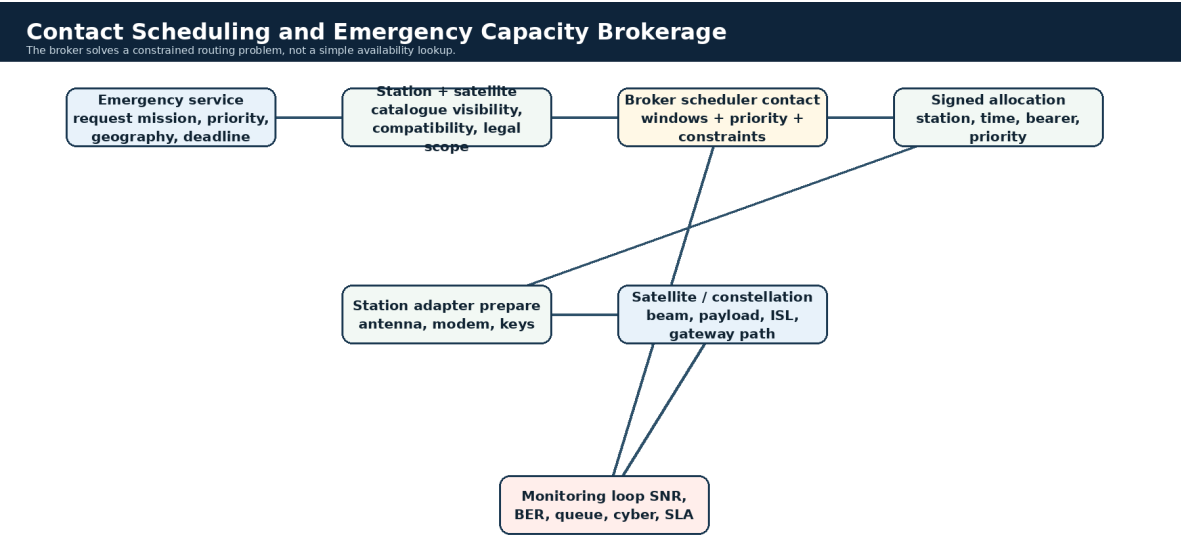


Figure 9. Contact scheduling and capacity brokerage workflow.

Constraint	Example	Scheduling consequence
Visibility	Satellite visible from station for 8 minutes	Allocate contact window and prepare station before AOS
Frequency/waveform	Station supports X-band but not required coding	Find compatible station or use onboard storage until compatible pass
Priority	Life-safety map product has higher priority than routine science data	Preempt or delay lower-priority downlink
Legal scope	Station can support humanitarian traffic but not foreign security traffic	Route only authorized service class
Cyber state	Station is trusted for receive-only but not uplink	Permit downlink, block telecommand
Backhaul	Station has satellite trunk only; fibre failed	Limit throughput and route via DTN queues
Weather	Ka-band site affected by storm	Switch to lower band, alternate site or lower coding rate

23.5 Telecommand risk separation

Telecommand is the highest-risk service in a ground-station federation. A station may safely receive telemetry or payload data for another operator, but transmitting commands introduces safety, liability and sovereignty implications. IFEGS should separate receive-only cross-support from command-capable cross-support. Receive-only services can be broadly pre-authorized. Command-capable services require mission-owner approval, sovereign approval when cross-border, dual control, validated command stacks, crypto key management and post-event audit.

Cross-support mode	Risk level	Recommended authorization
Payload data downlink	Low to medium	Pre-approved service descriptor and operator agreement
Telemetry receive	Medium	Mission owner approval; receive-only trust class

Cross-support mode	Risk level	Recommended authorization
Ranging/Doppler support	Medium	Mission owner approval and calibrated station data
Telecommand forwarding	High	Mission owner, station operator, national node and dual-person approval
Emergency spacecraft safing command	Very high	Pre-planned safing procedures, out-of-band verification and post-event review

24. Detailed Ground-to-Ground Connectivity Architecture

The connection between ground stations is not only a physical network. It is a layered federation of trust, routing, policy and service abstraction. The objective is to allow emergency traffic to use available infrastructure without merging institutional networks or exposing mission-control systems unnecessarily.

24.1 Recommended topology patterns

Topology	Description	Advantages	Risks / controls
Hub-and-spoke national node	Stations connect to national node; national node connects to regional broker	Strong sovereignty and policy control	National node becomes critical; needs redundancy
Regional broker overlay	National nodes exchange service requests through regional broker	Efficient cross-border coordination	Broker must not gain unauthorized control
Peer-to-peer station emergency tunnels	Stations establish pre-approved tunnels for specific services	Fast for pre-planned partner pairs	Must be narrow, logged and revocable
DTN store-and-forward mesh	Nodes store data until links become available	Resilient to outages and intermittent paths	Latency; requires prioritization and storage policy
Clean-core star	Compromised domains route only through clean-core services	Limits cyber spread	Reduced capability; must be pre-tested

24.2 API and message-bus design

The most convenient technical approach is to avoid direct database-to-database and station-to-station exposure. Each participating organization should publish an emergency API and message-bus endpoint through an adapter. Requests and responses should use signed messages, schema validation, replay protection and explicit mission identifiers.

Interface	Purpose	Minimum fields
Service discovery API	Find available station/service capabilities	Station ID, service type, legal scope, trust state, availability
Capacity request API	Request emergency capacity	Incident ID, priority, geography, service, duration, data sensitivity
Allocation response API	Provide route/contact allocation	Station, time, bearer, QoS, conditions, expiry, audit ID
Trust status API	Exchange cyber and operational trust state	Entity ID, state, reason code, expiry, confidence
Data request API	Access disaster data under policy	Requester, purpose, data class, scope, TTL, retention
Audit API	Submit signed evidence of actions	Actor, action, timestamp, cryptographic proof, result

24.3 Routing and QoS

Emergency routing should not rely solely on shortest path or lowest latency. The route selection function should optimize for mission priority, trust state, legal permission, performance, diversity and resilience. The routing engine should maintain independent paths for life-safety services, public warning, EO products, operational command and routine traffic.

Routing factor	Weight during normal operations	Weight during emergency
Latency	High for interactive services	High for command, lower for maps and EO
Throughput	High for broadband	Secondary to life-safety priority
Trust state	High	Highest
Legal authorization	Mandatory	Mandatory; emergency clauses may accelerate
Geographic diversity	Medium	High to avoid shared hazard zones
Power autonomy	Medium	High in grid failure
Weather resilience	Medium	High during cyclones/floods
Cost	Medium to high	Lower priority than life safety but still logged
Operator neutrality	Medium	High in security-sensitive contexts

25. Multi-Orbit, D2D, HAPS and Terrestrial Integration

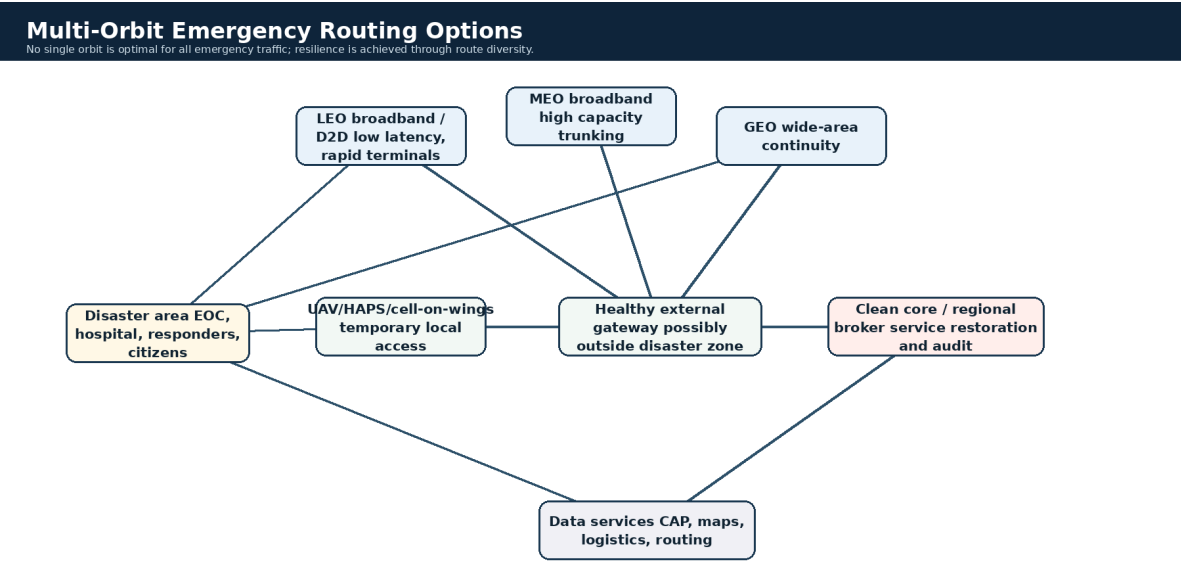


Figure 10. Multi-orbit routing and terrestrial restoration options.

The optimal emergency architecture uses all available communications layers. GEO remains valuable for wide-area continuity and broadcast. MEO offers high-capacity trunking with lower latency than GEO. LEO offers low-latency broadband and rapidly deployable terminals. Direct-to-device satellite can reach ordinary phones for messaging and warning. HAPS and UAV relays can restore local access. Terrestrial fibre, microwave and public-safety radio remain essential wherever intact.

25.1 Multi-orbit routing rules

Traffic type	Preferred primary	Preferred alternate	Contingency
CAP public warning	Cell broadcast / terrestrial alerting	D2D satellite / GEO broadcast	Radio/siren/community relay
Responder voice	Public-safety LTE/radio	LEO/MEO SATCOM	L-band satellite phone
Hospital data	Terrestrial fibre/microwave	MEO/LEO backhaul	GEO VSAT with priority QoS
EO downlink	Compatible ground station nearest product chain	Regional station with DTN relay	Onboard storage until clear pass
Shelter internet	Terrestrial mobile if restored	LEO hotspot / MEO backhaul	Low-rate GEO/L-band for essential services
Critical infrastructure telemetry	Private fibre/radio	Satellite IoT / L-band	Store-and-forward DTN

25.2 Direct-to-device satellite integration

D2D should be treated as a low-rate, high-value layer. It should not be planned as a substitute for full cellular service in a dense disaster zone. Its best use is public warning, distress messaging, responder backup messaging, registration of isolated survivors, and low-rate government continuity messages. Emergency D2D profiles should support priority, geographic targeting, multilingual templates and graceful fallback from richer data to short text.

25.3 HAPS and UAV relay integration

HAPS/UAV relay assets can act as temporary cellular or Wi-Fi islands with satellite backhaul. Their operational use requires pre-cleared airspace procedures, spectrum coordination, payload security, endurance planning, weather limits and clear authority for deployment. They are especially useful when terrestrial towers are physically destroyed but user devices remain operational.

26. Cyber-Physical Failure Modes and Defensive Playbooks

Cyber and physical failures often occur together. A storm can damage fibre while attackers exploit the confusion. A cyberattack can disable management systems while operators are under pressure from a natural disaster. A good playbook must treat blended failure modes as expected scenarios.

Failure mode	Symptoms	Immediate response	Restoration condition
Gateway power loss	Station offline, local alarms, generator status uncertain	Switch traffic to alternate gateway; dispatch power support if safe	Stable power + cooling + monitoring restored
Fibre cut	Satellite link healthy but no external routing	Use satellite trunk, microwave, DTN or alternate terrestrial carrier	Diverse backhaul validated
Modem compromise	Unexpected reboot, abnormal configs, suspicious commands	Isolate modem, revoke keys, reimage from golden image	Clean firmware and key rotation complete
Credential compromise	Unusual login/service requests	Disable account, revoke tokens, enforce emergency identity proof	Root cause found and accounts rotated
Jamming	SNR drop, interference signatures, geography correlation	Switch band/beam/site/orbit, collect spectrum evidence	Interference mitigated or alternate path stable
GNSS timing failure	Timing alarms, location inconsistency	Switch to holdover oscillator/PTP/alternate timing	Trusted timing restored
Database corruption	Conflicting maps/status records	Freeze updates, revert to signed snapshot, verify provenance	Integrity proof and reconciliation complete
AI routing error	Unsafe or unexplained recommendation	Fallback to deterministic rules and human review	Model review and rule update complete

26.1 Cyber incident phases

Phase	Objective	Operational rule
Preparation	Make compromise survivable	Clean-core drills, backups, pre-issued emergency keys, segmentation
Detection	Find compromise early	SOC/SIEM, anomaly detection, integrity monitoring
Containment	Stop spread and protect life-safety services	Quarantine suspect nodes; preserve P0-P2 communications
Eradication	Remove attacker access	Reimage, patch, rotate credentials and keys
Recovery	Restore services safely	Staged re-entry, heightened monitoring, user validation
Lessons learned	Improve architecture	Update EGSD, playbooks, contracts and exercises

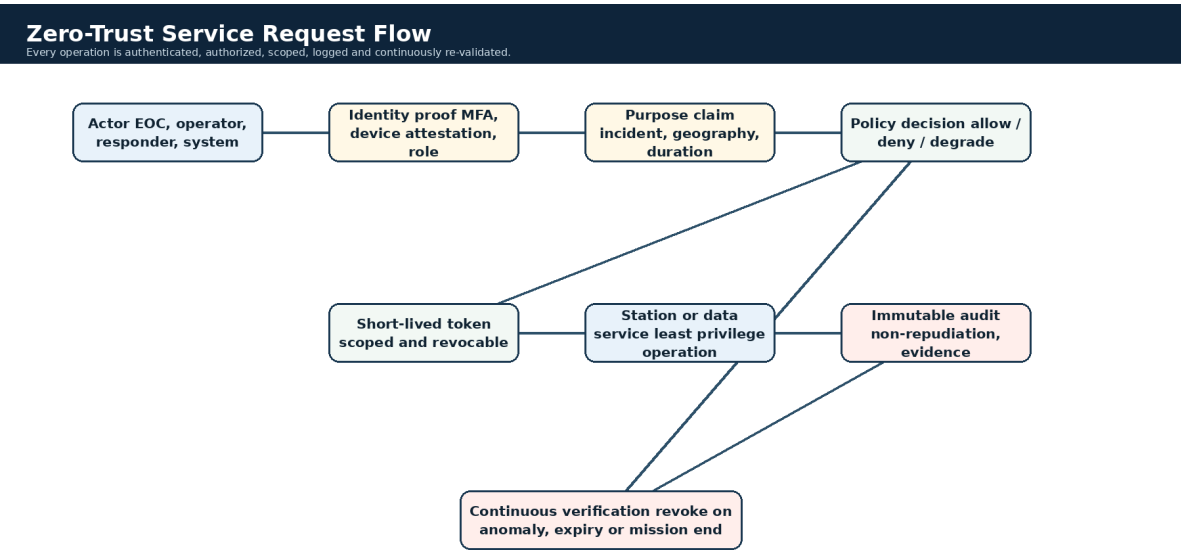


Figure 11. Zero-trust request flow for station and data services.

27. Regional Implementation Models

A global architecture must adapt to regional geography, hazard profiles, infrastructure maturity and legal culture. The following regional models are proposed as implementation templates, not geopolitical rankings.

Region type	Hazards	Architecture emphasis	Priority pilots
Continental high-infrastructure region	Floods, wildfires, heat, cyber crises	Integration of national nodes, secure government connectivity, telecom operators and EO services	Regional broker + public warning + cyber clean-core exercise
Island and coastal region	Cyclones, tsunamis, submarine cable failure	Pre-positioned terminals, D2D, GEO/LEO backhaul, maritime links	Island clean-core + D2D public warning pilot

Region type	Hazards	Architecture emphasis	Priority pilots
Seismic belt	Earthquakes, landslides, tsunamis	Rapid failover, mobile gateways, HAPS/UAV, station diversity outside hazard zone	Earthquake/cyber blended exercise
Large rural/remote region	Floods, droughts, wildfire, weak terrestrial networks	Satellite IoT, D2D, low-cost terminals, community radio	Rural public warning + health connectivity pilot
Security-sensitive region	Hybrid threats, jamming, cyberattack, cross-border tension	Civil/security separation, interference monitoring, protected data flows	Protected humanitarian corridor communications pilot

27.1 National architecture template

- Create a national emergency ground-segment authority or assign the role to an existing telecom/space/civil-protection coordination body.
- Build a national asset registry covering ground stations, teleports, gateways, mobile terminals, public-safety nodes and critical data services.
- Define national emergency priority classes aligned with public warning, life safety, healthcare and critical infrastructure restoration.
- Establish at least two physically and administratively diverse routes for national EOC connectivity.
- Designate a clean-core environment with independent identity, backup, logging and out-of-band communications.
- Conclude emergency service agreements with domestic and foreign satellite/ground-station providers.
- Run a national live exercise at least annually and a regional exercise at least every two years.

27.2 Regional broker template

- Maintain a regional catalogue of pre-approved emergency services published by national nodes.
- Operate a 24/7 broker desk and automated capacity request API.
- Maintain a regional legal matrix for temporary spectrum, terminal import, cross-border routing and data sharing.
- Coordinate regional exercises, including cyber/physical compound scenarios.
- Hold no unnecessary sensitive data; broker metadata and service requests only.
- Provide conflict-resolution procedures when multiple countries request limited capacity simultaneously.

28. Institutional Roles and Responsibility Matrix

Actor	Responsibilities	Must not do
National civil protection authority	Declare emergency, validate public warnings, set operational priorities	Bypass cyber/data controls without legal basis
Telecom regulator	Emergency spectrum, operator coordination, public warning compliance	Delay urgent temporary authorization unnecessarily
National space agency	Ground-station registry, space mission coordination, cross-support standards	Expose mission-control systems without safeguards
Satellite operator	Provide capacity, station data, terminals, cyber status and SLAs	Make unilateral sovereign/public-warning decisions
Ground-station operator	Publish EGSD, maintain station readiness, execute allocations	Accept unauthorized command or sensitive data tasks
SOC/CERT/CSIRT	Cyber monitoring, revocation, incident response and re-entry approval	Restore compromised systems without evidence
Regional broker	Match demand/capacity, escalate legal/security exceptions	Command national assets directly
Humanitarian organizations	Field connectivity, needs assessment, last-mile communications	Collect/share excessive personal data
International organizations	Standards, exercises, legal model clauses, global coordination	Centralize sensitive national databases

29. Verification, Validation and Certification

A contingency plan is only credible if tested. Certification should verify technical interoperability, operational procedures, cyber resilience, legal readiness and human performance. Paper compliance is insufficient.

Test type	What is tested	Pass criterion
Interface conformance	EGSD, APIs, service descriptors, trust messages	Schema-valid signed exchange with negative-test handling
RF/link test	Antenna/modem/waveform compatibility and link margin	Successful contact under nominal and degraded profiles
Failover drill	Primary path failure to alternate/contingency path	Service restored within defined time objective
Cyber tabletop	Ransomware, credential compromise, trust revocation	Clean-core activation and safe continuity of P0-P2 traffic
Live cyber range	Simulated malware/jamming/spoofing against testbed	Compromise contained; evidence preserved
Database access drill	Purpose-bound request and cross-domain redaction	Access granted/denied correctly and logged
Public warning simulation	CAP message routing through multiple channels	Message delivered, localized, logged and cancelled correctly
Human factors exercise	Shift handover, fatigue, conflicting authorities	No unresolved authority conflict; checklist completion
Legal drill	Temporary spectrum/cross-border approval	Decision reached within target time with documented authority

29.1 Maturity model

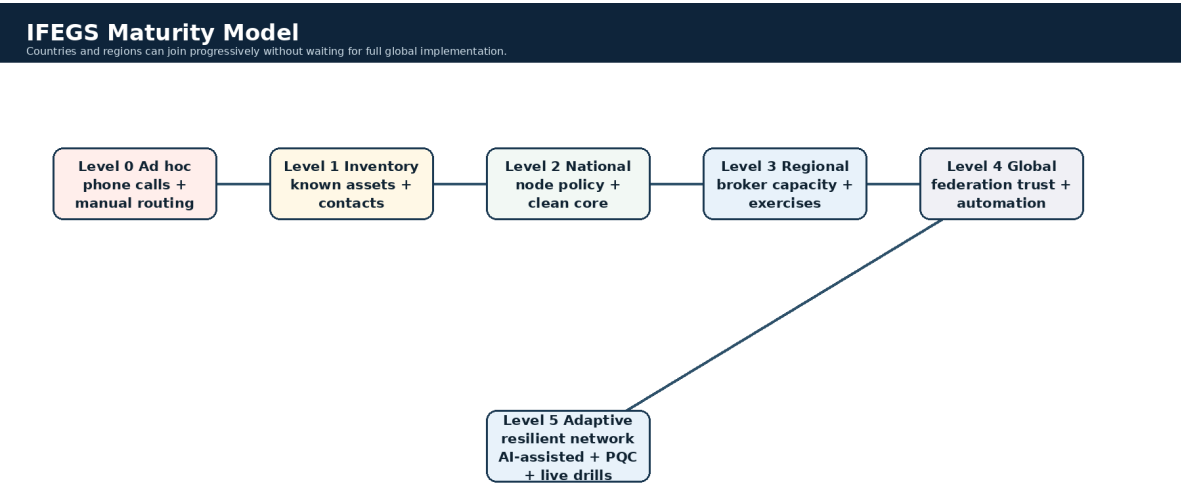


Figure 12. IFEGS maturity model from ad hoc response to adaptive resilient network.

30. Procurement and Industrial Policy Considerations

The recommended architecture should avoid vendor lock-in and single-provider dependence. Procurement should emphasize open interfaces, exportable logs, documented emergency APIs, multi-orbit compatibility, sovereign key control options, escrowed configuration baselines, cyber certification and interoperability testing.

Procurement requirement	Reason
Support for open emergency service descriptors	Allows regional brokers to discover and use capacity
Documented APIs and logs	Supports audit and after-action evidence
Multi-bearer support	Avoids dependence on one orbit, one band or one operator
Hardware roots of trust / HSM integration	Protects credentials and command paths
Offline and degraded modes	Keeps services alive during cyber or backhaul outages
Configuration export and golden-image recovery	Accelerates recovery from misconfiguration or malware
Interoperability test participation	Prevents paper-only compliance
PQC migration roadmap	Avoids stranded cryptographic infrastructure
Data sovereignty controls	Prevents uncontrolled data replication or foreign processing
Transparent emergency pricing/SLA	Prevents negotiation delays during crisis

31. Financing and Sustainability Model

Emergency ground-segment interoperability cannot rely only on post-disaster goodwill. It requires sustained funding for registries, exercises, clean-core infrastructure, standby capacity, terminal pre-positioning, cybersecurity, legal preparation and training. A mixed financing model is recommended.

Funding source	Best suited for	Notes
National budget	Sovereign node, public warning, clean core	Core capability should be nationally funded
Regional funds	Broker, cross-border exercises, shared terminal pools	Useful for river basins, seismic regions and island groups
Development finance	Low-connectivity regions, rural warning systems, training	Should include maintenance and local capacity-building
Commercial SLAs	Standby satellite capacity and emergency service products	Requires transparent activation and compensation rules
Insurance/resilience funds	Critical infrastructure continuity	Could incentivize tested resilient architectures
Humanitarian funding	Field terminals, shelter connectivity, community access	Should align with data-protection and neutrality principles

32. Policy Recommendations

Recommendation	Priority	Responsible actors
Develop the EGSD standard as the first technical deliverable	Immediate	CCSDS/ITU/OASIS/industry coalition
Create national emergency ground-segment registries	Immediate	National space/telecom/civil protection authorities

Recommendation	Priority	Responsible actors
Establish regional capacity broker pilots	High	Regional organizations and participating states
Pre-negotiate emergency satellite/ground-station SLAs	High	States, operators, humanitarian agencies
Mandate clean-core continuity for critical ground infrastructure	High	Regulators, operators, cybersecurity authorities
Define emergency priority classes for satellite/terrestrial convergence	High	ITU, 3GPP liaison, national regulators
Adopt purpose-bound secure disaster data exchange rules	High	Data protection authorities, civil protection, health agencies
Run annual cyber-physical failover exercises	High	All national and regional participants
Integrate D2D and NTN into public warning policy	Medium-high	Telecom regulators, mobile operators, satellite operators
Create a legal model clause package for cross-border emergency ground support	Medium-high	International institutions and legal working groups

33. Draft Institutional Action Plan

Month	Action	Output
0-3	Create founding working group and agree scope	Terms of reference and stakeholder map
3-6	Draft EGSD, priority classes and legal model clauses	Version 0.1 standards package
6-9	Select pilot countries/regions and participating operators	Pilot architecture and test plan
9-12	Deploy national node prototypes and clean-core testbeds	Operational demo environment
12-18	Run first tabletop and technical failover exercise	After-action report and standard updates
18-24	Run first live regional capacity brokerage test	Validated regional broker and API updates
24-36	Expand to inter-regional exercise and certification scheme	Maturity model and certification handbook

34. Final Institutional Position

The proposed IFECS concept is technically feasible because it builds on existing standards and operational practices. Its difficulty lies in governance, legal pre-clearance, trust, cyber resilience, commercial alignment and exercising. The most convenient path is therefore incremental but disciplined: standardize service descriptors, create national nodes, pilot regional brokers, require clean-core operations and certify participating assets through repeated cyber-physical drills. In this model, emergency communications resilience becomes a standing international capability rather than a post-disaster improvisation.

PART VII

SUPPLEMENTARY INSTITUTIONAL ANNEXES

Operational, legal and conformance material retained from the original contingency-plan version.



Supplementary Institutional Annexes Integrated from the Original Contingency Plan

The following annexes preserve material from the original contingency-plan version that adds distinct operational, legal, governance or conformance detail beyond the main technical manuscript. Repeated executive material and duplicated architecture descriptions have been intentionally omitted to keep this integrated master version coherent.

Annex D - Expanded Threat and Failure Model

IFECS assumes concurrent failures, because real crises combine physical damage, congestion, misinformation, software faults and human error. It therefore treats loss of connectivity and loss of trust as separate failure classes.

Threat / failure	Examples	Required architectural response
Physical	Earthquake, flood, wildfire, antenna damage, power/cooling loss	Geographic diversity, mobile terminals, autonomous power, alternate sites.
Telecom	Fibre cut, exchange outage, peering failure, cellular collapse	Multi-carrier terrestrial backhaul plus satellite PACE routes.
Space link	Rain fade, interference, jamming, satellite outage, ephemeris error	Band/orbit diversity, adaptive link selection, spectrum monitoring, DTN.
Cyber	DDoS, ransomware, wiper, credential theft, API abuse, supply-chain compromise	Zero Trust, segmentation, HSMS, signed artifacts, isolation, immutable logging, tested recovery.
Navigation/timing	GNSS jamming/spoofing or time-source corruption	Multi-source timing, holdover clocks, authenticated PNT where available, anomaly detection.
Data	Corrupt database, stale map, poisoned model, falsified telemetry	Provenance, signatures, confidence scores, versioning, independent corroboration.
Human	Misconfiguration, wrong tasking, accidental deletion, phishing, fatigue	Dual control, least privilege, runbooks, simulation, reversible actions and safe defaults.
Governance	No permission, export/customs delay, spectrum conflict, unclear liability	Pre-negotiated treaties/MOUs, emergency licences, contractual clauses and national decision authority.

Annex E - Global, Regional and National Operating Model

Global level

- Maintain common interoperability specifications, trust-policy templates and a distributed service catalogue.
- Provide a 24/7 global coordination mechanism for catastrophes spanning multiple regions or requiring scarce satellite capacity.
- Maintain emergency contact and spectrum/licensing information in coordination with ITU mechanisms.
- Coordinate humanitarian, civil and commercial capacity without assuming operational command over national assets.
- Publish conformance profiles and organize multinational exercises.

Regional level

- Operate Regional Emergency Capacity Brokers hosted redundantly in at least two participating countries.
- Maintain cross-border fibre/satellite failover maps, language/alert profiles and regional operator contracts.
- Perform regional cyber correlation while respecting national classification restrictions.

- Coordinate common disaster scenarios such as Mediterranean floods, Caribbean cyclones, Asia-Pacific earthquakes/tsunamis, African transboundary floods and European cross-border infrastructure disruptions.

National level

- Designate one national authority for emergency communications policy and one technical operating function; these may be institutionally separate.
- Maintain the authoritative asset registry, emergency licences, operator agreements, contact tree and national data-sharing rules.
- Pre-stage portable satellite/mesh/energy kits in hazard-relevant regions.
- Conduct annual failover exercises including loss of the national primary data centre and primary satellite operator.
- Ensure national operation is possible while disconnected from regional/global services.

Annex F - Japan-Type Earthquake and Tsunami Warning Scenario

Situation: a severe earthquake damages terrestrial networks in coastal and mountainous areas. Japan's QZSS disaster/crisis report service illustrates how satellite warning can complement terrestrial networks: QZSS transmits disaster information over L1S and extended services include J-Alert/L-Alert information, with regional expansion work in Asia-Pacific. [13]

16. Authoritative national warning is generated and signed.
17. Terrestrial cell broadcast and sirens remain primary where available; satellite warning provides an independent path.
18. National ground assets prioritize emergency traffic, while portable satellite links restore EOC and hospital backhaul.
19. Regional assistance is requested only for capacity shortfalls or destroyed gateways.
20. Public alert services remain logically separated from sensitive emergency-command networks.

Annex G - Expanded Legal and Regulatory Framework

This section is a policy-engineering analysis, not legal advice. Detailed implementation requires jurisdiction-specific review.

Tampere Convention

The Tampere Convention, in force since 2005, is the most directly relevant treaty for international disaster telecommunications. It calls for prompt telecommunication assistance and reduction/removal of regulatory barriers such as equipment import/export restrictions, radio-spectrum restrictions, personnel movement and transit delays. It also preserves the affected State's right to direct, control and coordinate assistance within its territory. As of September 2026, the UN Treaty Collection records the Convention and ITU reports 50 ratifications following Saudi Arabia's 2025 ratification. This means the Convention is valuable but not universal. [14–15]

ITU Radio Regulations and emergency spectrum

ITU Radio Regulations remain the international framework for spectrum use. Resolution 647 addresses spectrum-management guidance for early warning, disaster prediction, detection, mitigation and relief, and ITU maintains emergency contact/frequency information submitted by administrations. IFECS should build a machine-readable policy layer on top of these national submissions, but cannot override national licensing or international frequency allocations. [2–3]

Outer Space Treaty and state responsibility

The Outer Space Treaty establishes international responsibility for national space activities, including those of non-governmental entities, and requires authorization and continuing supervision by the appropriate State. It also preserves jurisdiction and control over registered space objects and calls for cooperation, mutual assistance and due regard. Consequently, an emergency federation should never imply that a foreign broker acquires command authority over another State's or operator's spacecraft merely because connectivity is needed. [16]

Cybersecurity and critical-infrastructure law

In the EU, NIS2 expressly covers operators of ground-based infrastructure supporting space-based services, subject to its defined scope and exclusions. The proposed EU Space Act (2025 proposal, still legislative rather

than final law as of September 2026) seeks harmonized requirements on safety, resilience and sustainability. These frameworks point toward stronger mandatory cyber-risk management for ground segments but remain regional rather than global. [17–18]

Data protection, sovereignty and evidence

- Personal data and sensitive operational data should remain subject to applicable national/regional data-protection laws even during emergencies unless a lawful emergency basis applies.
- Cross-border data requests should specify purpose, scope, retention and recipient. Emergency access should expire automatically.
- Logs may become evidence in cyber, safety or liability investigations; therefore time synchronization, integrity and chain-of-custody controls are required.
- Data-localization laws may prohibit bulk replication; federated query patterns reduce this legal friction.
- Commercial licence terms, export controls, sanctions and security classifications must be represented in the policy engine as enforceable constraints, not informal notes.

Legal gaps requiring new instruments

Gap	Why existing law is insufficient	Proposed instrument
Emergency satellite/ground “roaming”	No universal right or framework for cross-operator emergency use.	Multilateral model agreement + bilateral/regional annexes; pre-negotiated capacity and liability.
Cross-border machine authorization	Treaties are generally written for human/organizational assistance, not automated federation.	Common legal profile for time-bounded machine credentials and automated routing.
Liability for misrouting/mis-command	Cross-support can create unclear allocation of responsibility.	Service-class liability matrix; strict separation of connectivity from command.
Cyber incident information sharing	Classification, privacy and commercial secrecy inhibit rapid sharing.	Protected emergency cyber-sharing protocol with minimum indicators and safe-harbor rules where legally feasible.
Emergency data access	No globally consistent rule for disaster access to critical datasets.	Purpose-bound data-sharing clauses and standardized emergency data categories.
Non-party states to Tampere	Convention benefits are not universal.	Regional mutual-assistance agreements adopting equivalent pre-clearance procedures.
Commercial continuity obligations	Emergency priority and capacity reservation differ by contract.	Standard emergency SLA clauses and public-interest priority tiers.

Annex H - International Working Group Decision Package

Decision required	Recommended position
Centralized vs federated architecture	Federated; global coordination must not become a mandatory transit point.
Default database model	Federated query/event exchange; no global replication of sensitive national databases.
Autonomy level	High for routing inside pre-authorized envelopes; low for privileged command and sensitive data release.
Cyber trust	Zero Trust + cryptographic identity + continuous posture; compromise of one member must not compromise federation.
Interoperability	Standards-first adapters; do not require replacement of legacy stations.
Commercial model	Pre-event framework contracts and emergency capacity reservations with transparent priority rules.

Decision required	Recommended position
Legal model	Tampere-compatible mutual assistance + regional/bilateral annexes + national sovereign approval.
Technology roadmap	Operational now with CCSDS/IP/DTN/satellite/terrestrial assets; progressively integrate NTN/D2D, optical, HAPS, AI and PQC.
Validation	Mandatory multinational exercises and independent red-team/cyber evaluation before operational certification.

Annex I - Suggested Conformance Levels

Level	Capability
L0	Asset inventoried; no federation interface.
L1	Publishes signed EGSD and health status.
L2	Supports authenticated capacity request and read-only data exchange.
L3	Supports automated PACE failover for non-privileged services.
L4	Supports cross-border/regional brokerage and cyber isolation/rejoin.
L5	Advanced autonomous operation with independent assurance, multi-orbit/NTN integration and crypto agility.

Integrated Master Conclusion

This master document consolidates the technical reference architecture and the original contingency-planning material into one institutional baseline. The main body provides the preferred federated technical architecture; the supplementary annexes retain distinct threat-model, operating-model, legal, scenario, decision-package and conformance content that may be useful for international working groups, standards bodies, regulators, civil-protection authorities and security stakeholders.