



Open Discussion #2

BARCELONA
2025

Complexity of Building Robust and Resilient Systems

Moderators

Prof. Dr. Petre Dini, IARIA, USA/EU

Prof. Dr. Eugen Borcoci, National University of
Science and Technology POLITEHNICA
Bucharest, Romania



Petre Dini
IARIA, USA/EU



Eugen Borcoci
NUST
POLITEHNICA, RO

Robustness = don't fall easily, endure and deliver (**withstanding disturbance**)

Resilience = get up quickly, recover fast and cleanly when you do. (**recovering gracefully**)



Open Discussion #2

BARCELONA
2025

- **Robustness** (early phase, prevention by design, redundance, preventive maintenance)
 - Ability to maintain operational functionality under a range of conditions, pressures, or stresses
 - Strength and stability, ensuring the system can withstand external disruptions without significant performance degradation
- **Resilience** (after, exception handling, risk mgmt, by design, enforced, customized mechanisms)
 - Capability to recover quickly from difficulties, adapting effectively to significant changes or disruptions
 - Flexibility and recovery, enabling a system to return to its original state or evolve into a new, functional state following a disturbance.
- **Quick outcome**
 - Design, resources, planning, budgets, law enforcement, risk management, training, awareness
 - Human behavior (designer, control and management, user)
 - Interagency cooperation (governments, police, administration, stakeholders, owners, service providers)
 - Large spectrum of approaches for enabling the robustness ability and resilience capability, for each kind of system
 - Technology seems the least obstacle
 - Mostly humans and Rule of Laws; since, AI-based tools cannot Do much, but speeding a resolution.



Open Discussion #2

BARCELONA
2025

■ Robustness

- (a) Redundancy (software/hardware/grid/systems failure)
- (b) Solid levees (from flooding)

■ Resilience

- (a) Quick switch (cold/warm/hot standby) (state transfer)(load balance)
- (b) Easy and clear administrative rules and actions for cleaning the flooded area and reinstalling the levees.

Q: After robustness fails **the duration** until the full resilience takes effect may affect many lives, services, etc.

Risk assessment indicates how much **effort** (**budget, time, personnel**) should be put for robustness and **how complex and costly** the resiliency capabilities should be until a system recovers with minimum loss.

Affordability vs **Estimated risk** vs **Accepted loss**



Open Discussion #2

BARCELONA
2025

■ Industrial Chain systems

- **Resilience:** Adaptive supply chains, regulatory compliance, financial stability, long-term environmental considerations and risk assessment
- **Robustness:** (continuous service) Supply chain disruption control, (allows) quality control variability, (avoid) technological obsolescence, (combat) cybersecurity threats

■ Agriculture Crops systems

- **Resilience:** Climate adaptation, economic viability, Technological integration, community and knowledge sharing
- **Robustness:** (via) Pest and disease management, (monitor) Soils health, (control) Water Management, (assure) Genetic diversity

■ Agriculture livestock systems

- **Resilience:** Breeding, Biosecurity, Market flexibility, Resource management
- **Robustness:** (perform) Disease control, (select) Generic robustness, (avoid scarcity) Feed availability, (assure) Housing and infrastructure, (posses) Medical assistance

Robustness (preparative actions, redundancy) endure and deliver & withstand external disruptions

Resilience: (mechanisms) flexibility to recover from significant changes or disruptions



Open Discussion #2

BARCELONA
2025

■ Political system

- **Resilience:** Adaptive to change (crisis, social movements, market), Institution redundancy (to continue under stress), Social cohesion (national identity), International relations
- **Robustness:** Corruption, Transparency, Rule of law, Citizen political participation, media freedom,

■ Social systems

- **Resilience:** Strong community networking, adaptive governance, social mobility, communication channels
- **Robustness:** Economic inequality, healthcare accessibility, education disparities, institutional trusts

■ Firefighting systems

- **Resilience:** Mental health support, interagency cooperation (police, health etc.), community engagement and preparedness, adaptation (climate, wildfires)
- **Robustness:** Aging infrastructure (machinery), Technology integration, Training and preparedness, Funding and resource allocation

Robustness (preparative actions) endure and deliver & withstand external disruptions

Resilience: (mechanisms) flexibility to recover from significant changes or disruptions



Open Discussion #2

BARCELONA
2025

■ Airport systems

- **Resilience:** Emergency response, Recovery (crisis), capacity and flexibility (for surge in numbers) and maintaining the QoS, sustainability practices (environment), stakeholder communication (govt, airlines, service providers)
- **Robustness:** Infrastructure vulnerabilities (runways, terminals, air traffic control towers), cybersecurity threats (flight schedules, security systems), interdependencies of systems (baggage handling, fuel supply), compliance with regulations

■ Disability systems (in Cities)

- **Resilience:** Emergency preparedness, adaptive urban planning, unforeseen traffic disruption, vulnerability to extreme weather, elderly reduced mobility
- **Robustness:** Accessibility and mobility (universally accessible sidewalks, crossings, and public transit options), consistent service provider (healthcare, education, and social support), assistive technologies into public infrastructure, enforcing policies that mandate accessibility (across different areas)

■ Disability systems (in an Airport)

- **Resilience:** Crisis mgmt. (evacuation), service continuity (wheelchair assistance and priority boarding), adaptive policies (feedback from disabled travelers), coordination (airlines, airport authorities, and ground service providers)
- **Robustness:** Inclusive design (from check-in to boarding), staff training and awareness, assistive technologies (malfunctioning wheelchairs or inadequate hearing loop systems), accessibility (braille, large print, and audible info)



Case Study | AWS disruption, Oct 20, 2025

BARCELONA 2025

Amazon web services return to 'normal operations' after mass outage, tech giant says

© 20 October 2025

First, the outage originated in AWS's northern Virginia cluster, known as US-EAST-1, which is the world's largest cloud provider.

Second, we know the Domain Name System (DNS) is also the likely cause of the fault. Likened to the internet's "phone book", the DNS can "paralyse" entire applications and services if its domain name resolution stops working, according to experts.

The root of the problem was a malfunction at Amazon Web Services, the tech giant's cloud computing division, whose infrastructure underpins millions of large companies' websites and platforms.

The outage hit early today, and affected companies as varied as Snapchat, Roblox, Zoom, Coinbase, HMRC and even banking services like Lloyds, Bank of Scotland and Halifax

... both the Roblox game and the development tool went down for many developers, both in the UK and in the US.

Reports of apps being down started at 08:00 BST, and Downt detector told the BBC it had received reports stating it got 6.5 million reports and over 1,000 companies were facing problems

But problems persist, including with its Lambda service, which computer science experts say helps ensure your cell phone, computer, or television can run apps from the cloud.

Though a "seemingly minor piece of infrastructure", Szustak points out that DNS can "paralyze" the largest cloud environments.

Consumer champion Matt Allwright warns that scammers could take advantage of people during an internet outage.

Popular financial apps like Venmo and Coinbase are still experiencing problems. Gaming giants like Roblox and Fortnite were impacted but are back up and running.

Downdetector now says users have been reporting issues with Grok, Lyft, Claude AI, Hulu and Reddit in updates posted on its X account. Educators struggle as Canvas service interrupted



Common DNS trouble-causes in AWS

BARCELONA
2025

When DNS breaks, everything follows quickly— even in infrastructures as hardened as AWS.

Classical paradox: the service most fundamental to resilience is often **the single point** whose **failure** cascades universally.

Conclusion: **robustness** (redundant design) doesn't automatically ensure **resilience** (graceful recovery).

Regardless the scale of cloud, **DNS** is still globally synchronized, time-sensitive, and cache-fragile.

1. DNS resolution / throttling limits

AWS's VPC-provided DNS resolver limits queries per elastic network interface (ENI). If you exceed ~1,024 packets/second you may see DNS timeouts/drop.

2. Misconfigured name server / hosted zone settings

Examples: wrong NS records at registrar, or multiple hosted zones with the same domain name confusing resolvers

3. Partial failures / resolver caching issues

A name may resolve publicly but fail internally (or vice versa) because of private vs public zones, or stale caches/TTL delays.

4. Network / VPC connectivity issues

If the EC2/VPC cannot reach the DNS server (private resolver or Route 53 resolver endpoints) due to mis-routed subnets, NAT gateways missing, firewall/security group mis-configurations, then DNS fails.

5. DDoS or internal subsystem failure

A DNS-system overload or failure (even within AWS's internal infrastructure) can cause widespread DNS resolution outages. Example: recent AWS outage traced to DNS resolution failure.

6. Mis-routing between internal and external DNS zones

If you have private hosted zones that shadow public names, but records are missing for your internal queries, you may get “name not found” even though it works externally.

7. Time-to-live (TTL) & propagation issues

After changing DNS settings, old records may still be cached, causing inconsistent resolution.

Throttling limits are a mechanism that restricts the number of requests a client can make to a service within a specific time frame to prevent overload and ensure fair resource allocation. This can involve temporarily slowing down or rejecting subsequent requests once a pre-defined limit is reached, which helps maintain service stability and performance for all users.



DNS - AWS

BARCELONA
2025

Actions for Robustness

Preventive, structural measures that make DNS less likely to fail.

1. Redundant resolvers and paths — at least two independent DNS servers (preferably across regions and providers).
2. Zonal replication — duplicate hosted zones in multiple regions with automated sync.
3. Distributed caching — local DNS caches or edge resolvers to reduce dependence on upstream queries.
4. Rate control / query throttling — avoid overload of VPC or corporate resolvers.
5. Configuration validation — continuous checks for stale or inconsistent NS/A/CNAME records.
6. Isolation testing (“chaos DNS”) — simulate resolver loss to verify continued service.

→ **Goal: minimize the probability of DNS becoming a single point of failure.**

Amazon Route 53 is a scalable and highly available Domain Name System (DNS) web service that translates user-friendly domain names, like `www.example.com`, into numerical IP addresses, like `192.0.2.1`, which computers use to connect to each other. In addition to acting as a DNS service, Route 53 also offers domain registration, allows users to manage their public DNS names, and provides health checking to route traffic to healthy applications.

Mechanisms for Resilience

Dynamic, adaptive responses when failure still occurs.

1. Fail-over resolvers — clients automatically retry alternate servers (e.g., Route 53 → secondary provider).
2. Graceful caching / TTL management — longer TTLs for critical records so clients keep functioning during upstream outage.
3. Self-healing resolver clusters — health checks that detect and respawn failed DNS endpoints.
4. Dynamic rerouting / traffic steering — switch to known-good zones via automation or Anycast redirection.
5. Monitoring + alerting loops — detection within seconds and automated playbooks to isolate or restart faulty components.
6. Progressive re-propagation — staggered DNS record re-validation to prevent cache storms after recovery.

→ **Goal: minimize the impact duration and scope once failure happens.**



DNS - Causes and Remedy

BARCELONA
2025

What to check when you hit DNS troubles in AWS

- Check the DNS query rate from your VPC / ENI: are you hitting the limit?
- Validate that the hosted zone, NS records, and registration settings are correct.
- Ensure your VPC/subnet configuration allows traffic to the resolver (for private zones etc.).
- Test internal vs external resolution: do queries work from an EC2 inside the VPC?
- Monitor the AWS Service Health Dashboard / status page for regional DNS/resolver issues.
- Cache flush / increase retry timer on client side if intermittent timeouts.
- Consider adding a fallback DNS (public) for non-critical resolution paths if needed.

Robustness (preparative actions, redundancy) endure and deliver & withstand external disruptions

Resilience: (mechanisms) flexibility to recover from significant changes or disruptions



Case study - Communication Networks

BARCELONA
2025

Robustness(Rb) and Resilience (RI)- important characteristics of communication networks

In the networking area, Rb and RL are partially overlapping

Main objective

Robustness

Withstanding anticipated variations and operating under expected conditions:

traffic load, mix of different traffic classes

number of calls, multiple tenants (5G)

topology changes (mobile networks)

various QoS requirements

security/privacy issues

scalability (H/V, slice resources, scaling in 5G/cloud - based infrastructure, etc.)

various types of access to networks and services

real-time response for critical missions

Interworking of different technologies (local, access, aggregation, core)

Resilience

Recovering from and adapting to unanticipated disruptions

(the same problems as for robustness but quantitatively larger range of issues) +

SW failures

routing failures

security attacks (many types)

severe congestion

loss of centralized control (SDN)

topology segmentation,

some important functional control blocks

failures,

unacceptable slice interference (5G), etc.



Case study - Communication Networks

BARCELONA
2025

Primary function in networking

Robustness: Stability vs. expected challenges; maintain performance under known problems and variations

Resilience: Return to a functional state after a failure by recovering after unforeseen events

Robustness vs. resiliency

Robustness: it is supposed to be powerful enough in order to help the resilience

Resilience: usually, incorporates robustness as a key attribute

Note: The traditional management systems (defined in telecom long time ago) had objectives and functions related to both robustness and resiliency

The classic TMN functionalities: F: fault detection and solving, C: configuration, A: accounting, P: performance evaluation S: security

these principles are still valid but at an advanced approach

Today networks & services

- convergence of network architectures (IP-based technologies)
- extended softwarization
- many access technologies, multiple tenants, many apps. with novel services reqs.
- mobility: 5G, 6G (integrating terrestrial and spatial networks), IoT, IoV, UAV, etc.
- cooperation with Cloud/Edge/Hybrid computing : XaaS



Case study - Communication Networks

BARCELONA
2025

Novel M&C technologies (more flexible, powerful, adaptive, ..) - > more powerful Rb&RI

Policy Based Management, Cognitive/Autonomic management, novel AI supported functions in M&C
Virtualization, Software Defined Networking, Network Function virtualization, Orchestration arch.
plane, Failure-aware design (proactive approach)

Example: 5G Cloud-Native features- enhance both Robustness and Resilience

Key principles

Microservices architecture

Individual NFs are broken down into smaller, independently managed services.
The microservices communicate through APIs; seamless updates and scalability

Containerization

5G NFs are packaged in lightweight containers; easily portable across environments
Services can be deployed quickly and consistently, minimizing downtime

Automated orchestration

Typically managed by Kubernetes, which automates the deployment, scaling, and management of containers

Kubernetes also powers self-healing and auto-scaling; essential for maintaining reliability and optimizing resource use during periods of high demand



Open Discussion

BARCELONA
2025

STAGE IS YOURS

Robustness: (preparative actions) endure and deliver & withstand external disruptions

Resilience: (mechanisms) flexibility to recover from significant changes or disruptions