



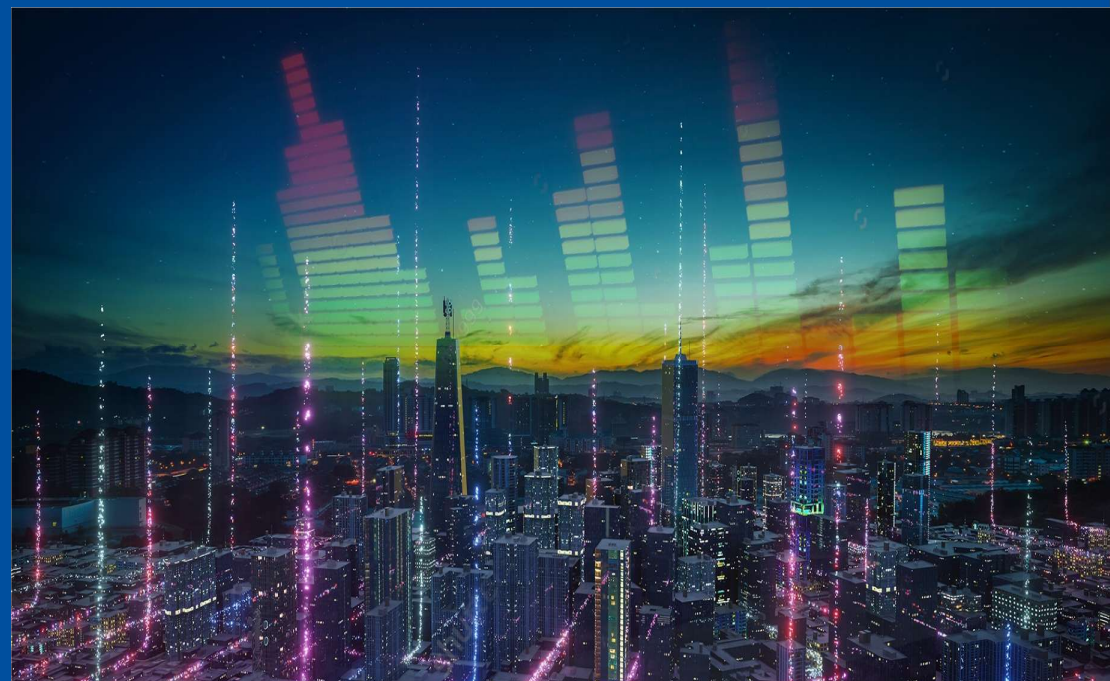
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBER STRESS TEST GAS SECTOR

NIS CG WS ON ENERGY 13TH PLENARY MEETING

Ricardo Figueiredo
ENISA Resilience of Critical Sectors Unit

09 | 10 | 2026





EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONCEPT, DESIGN, STRUCTURE AND DATA COLLECTION

09 | 10 | 2026

CYBER STRESS TEST – CONCEPT, OBJECTIVES, SCOPE

Scenario-based
“What-if?”

Resilience
focused

Stress levels

A cyber stress test is a targeted assessment of the resilience of individual entities and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios.

Resilience
metrics

Individual and
independent

Systemic
risk view

Objectives

- To provide evidence on the operational ability of entities in the gas sector to prevent, respond and recover from disruptive cyber scenarios
- To open a constructive dialogue between entities, authorities, regulators and other stakeholders – Not a supervision exercise

Scope

- EU level, TSOs and DSOs operating in the EU gas sector

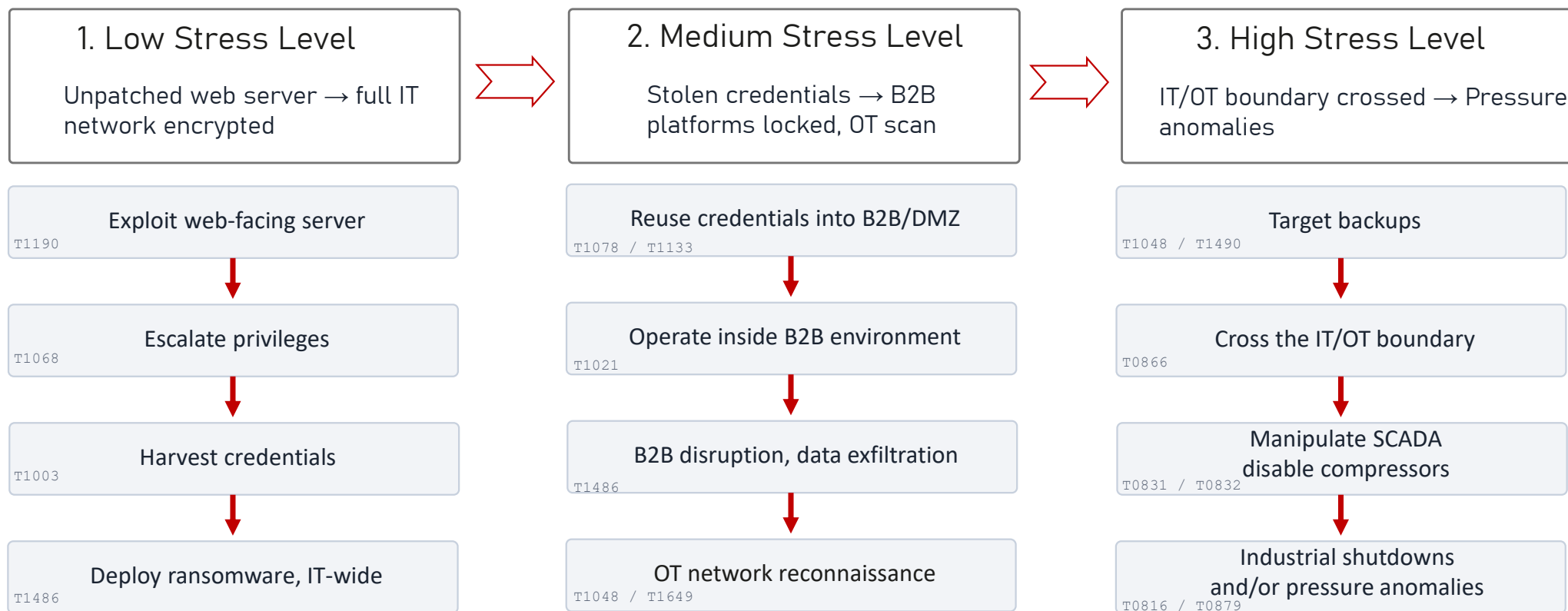
GAS SECTOR IMPLEMENTATION ASPECTS

- Lightweight approach – focus on not to overburden authorities
- Support from the NIS CG WS on Energy
 - Scenario design
 - Data collection – questionnaire sent directly to market operators
- Data was collected on key resilience areas
 - Prevention and detection;
 - Incident response;
 - Incident recovery
- Industry support - ENTSG as subject matter experts



SCENARIOS

3 scenarios, increasing stress level focusing on key assets (Corp IT, B2B platforms, and OT)



DATA COLLECTION STRUCTURE AND METRICS

40 questions, divided by 3 scenarios and 3 categories under each scenario

	CATEGORY	QUESTION (example)	RESILIENCE METRIC	RESILIENCE CAPABILITY
<u>1. Low Stress Level</u> Unpatched web server → full IT network encrypted	Prevention and detection	<i>What is the average time required to apply security patches to IT systems?</i>	Average time to patch IT systems	IT Vulnerability Management
	Incident response			
	Incident recovery			
<u>2. Medium Stress Level</u> Stolen credentials → B2B platforms locked, OT scan	Prevention and detection	<i>Describe the procedures used to coordinate incident response and crisis management, as well as which teams/units are involved</i>	Existence and maturity of a cross-functional incident response plan (IR plan maturity score)	Cyber Crisis Management Capability
	Incident response			
	Incident recovery			
<u>3. High Stress Level</u> IT/OT boundary crossed → Pressure anomalies	Prevention and detection	<i>What controls are in place to secure remote connectivity or privileged access to OT systems in distributed gas sites?</i>	% of OT remote access sessions protected by MFA, PAM, and session recording	Identity & Access Security Maturity
	Incident response			
	Incident recovery	<i>Does your organisation maintain offline or air-gapped backups for critical OT configurations and SCADA databases?</i>	% of critical OT configurations backed up offline / air-gapped	Critical Service Continuity

SAMPLE

CATEGORY	#	QUESTION TYPE	QUESTION	METRIC	RESILIENCE CAPABILITY	DESCRIPTION
PREVENTION&DETECTION	1	Multiple choice	Which security measures are implemented to protect your web facing apps and IT network? (select all that apply)	Number / % of security measures implemented on IT environments	Perimeter & Edge Security Maturity	Measures breadth of technical controls deployed (WAF, MFA, IDS, segmentation)
	2	Scale	On a scale of 1–10, rate the effectiveness of your perimeter defenses	Number / % of security measures implemented on IT environments		Self-assessed composite confidence in perimeter posture
	3	Multiple choice	What is the average time required to apply security patches to IT systems?	Average time to patch IT systems	IT Vulnerability Management	Measures how quickly the vulnerability window closes after a CVE is disclosed
	4	Quantitative	How frequently do you perform penetration testing on your corporate IT network? (Provide times per year)	Scope and frequency of pentesting on IT systems	Security Testing Maturity	Indicates how regularly and comprehensively security controls are adversarially validated.
	5	Multiple choice	What controls govern remote or privileged access to admin/system IT accounts? (Select all that apply)	Number / % of security measures implemented on IT environments	Privileged Access Management Maturity	Specifically measures access governance strength for high-value accounts
	6	Scale	On a scale of 1–10, rate your organization's ability to detect a ransomware infection in IT systems? What is the documented target or observed Mean Time to Detect (MTTD)? (Provide hours):	MTTD (Mean Time to Detect)	Threat Detection Capability	Time elapsed between intrusion and detection. Critical in ransomware scenarios where dwell time determines blast radius
INCIDENT RESPONSE	7	Scale	On a scale of 1–10, rate your organization's ability to contain ransomware a ransomware infection in IT systems before lateral movement occurs? What is your organisation's documented target or observed Mean Time to Contain (MTTC) a ransomware infection in IT systems? (Provide hours)	MTTC (Mean Time to Contain)	Incident Containment Capability	Time from detection to successful containment. The difference between a limited incident and catastrophic full-network encryption.
	8	Qualitative	If preventive measures fail, what incident response procedures are triggered following a ransomware attack? Who triggers the procedure, who is notified, in what order, and within what timeframes?	% of incidents mitigated without service disruption	Incident Response Maturity	Outcome metric measuring whether IR capability resolves incidents while maintaining operational continuity
INCIDENT RECOVERY	9	Quantitative	What is the defined Recovery Time Objective (RTO) for billing systems, and has this RTO been validated through a recovery test in the past 12 months?	RTO (Recovery Time Objective)	Business Service Recovery Capability	Maximum acceptable time to restore billing operations. Shorter RTOs require investment in recovery infrastructure and tested procedures
	10	Quantitative	What is the defined Recovery Point Objective (RPO) for corporate IT systems? How old is your most recent validated backup?	RPO (Recovery Point Objective)	Data Recovery Capability	Maximum acceptable data loss expressed as time
	11	Multiple choice	Are offline backups maintained for corporate IT systems?	% of systems backed up for rapid restoration	Backup Resilience	Coverage of offline backup across the IT estate. Systems without backups have no recovery path other than ransom payment



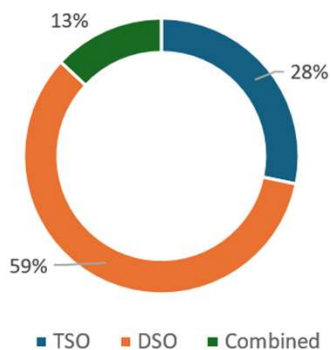
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PRELIMINARY RESULTS (NON EXHAUSTIVE)

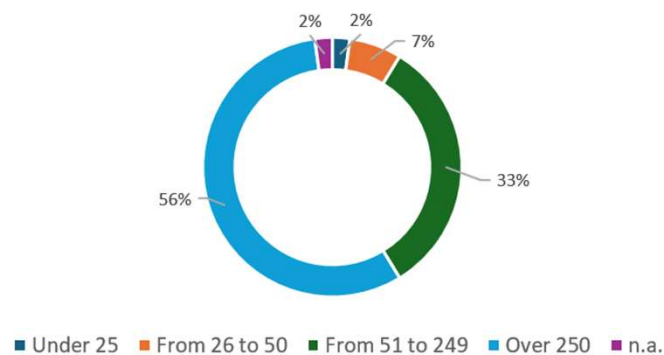
09 | 10 | 2026

POPULATION STATISTICS

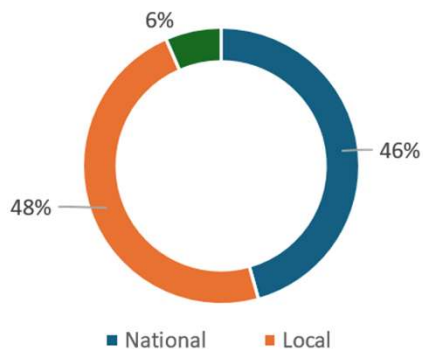
Type of Operator



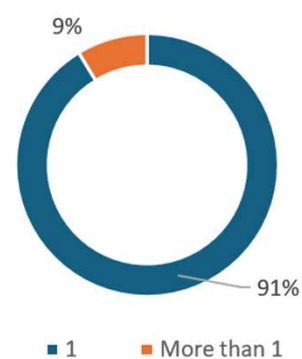
Number of Employees



Geographic Scope



of Countries of Operation



Other Questions	Average	Median
Lenght of pipeline network	10.541	1.322
# of compressor stations operated	33	-
# of interconnection points	23	3
# of remote/unmanned sites connected to SCADA	217	8
# of OT vendors with active support contracts	4	2
# dedicated information security/cybersecurity FTEs	7	2

OVERALL SCENARIO AND CATEGORY SCORE

Results fairly consistent across scenarios

	1. Low Stress Level		2. Medium Stress Level		3. High Stress Level
Prevention and Detection	6,8	→	6,5	→	5,9
Incident Response	6,9	→	4,5	→	6,6
Incident Recovery	6,0	→	6,3	→	6,9
	6,6		6,1		6,5

AT A FIRST GLANCE – WHERE RESILIENCE HOLDS

Low Stress Level

Perimeter defenses (Q1)

Strong 8.0/10

Pentesting (Q4)

Strong 6/10

Medium Stress Level

Network segmentation (Q12)

Strongest score 8.9/10

High Stress Level

SIS segregation from SCADA (Q36)

Strong 8.7/10

Manual compressor override (Q35)

half of operators report full capability

- The outer wall holds
 - Perimeter defenses (8.0) and defense in depth (8.7) all hold up well
 - Segmentation (Q12) is visibly strong —scores the highest (8.9)
- Manual operation of infrastructure seems to be there



AT A FIRST GLANCE – WHERE RESILIENCE WEAKENS

1. The access-control weak link and IT/OT interfaces

- Admin access control (Q5) is the lowest-scoring prevention control (5,6/10) in S1 – “facilitating” privilege escalation!
- B2B access controls (Q13) score weak (5,2/10)
- The OT remote access controls (Q26) scores the lowest of any critical control in the entire dataset (4,8/10)
- IT/OT boundary pentesting frequency (Q29) scores the lowest (4,6/10) in the whole S3 P&D category

2. Coordination and containment once the incident crosses internal boundaries

- Scenario 2 Incident Response is the lowest category score (4.5/10), while cross-operator procedures in Scenario 3 (Q33) are often untested or informal
- Over two dozen different incident-command structures reported across the 42 respondents (Q8)
- Just 1 in 5 have a response plan with both defined roles and a committed timeline (Q8)
- Fail safe mechanism for B2B platform isolation exists for 50% of respondents, but only 33% of those describe both the mechanism and the fallback (Q18)
- The isolation procedure and safe operating state — arguably the two most consequential controls lack supporting evidence. 1 in 3 operators could not describe their OT isolation procedure at all (Q31)



AT A FIRST GLANCE – WHERE RESILIENCE WEAKENS

3a. The documented-vs-tested gap - recovery of OT is potentially less mature than the scores suggests

- Only 4 in 10 could provide an actual number for SCADA recovery time (Q34)
- 66.7% of operators have never tested their OT safe-state restart procedure (Q37)
- Yet, 64% rate their confidence in a 7-day OT blackout at 8/10 or higher (Q39)
- RTO validation falls from 59% → 26% as you move from IT to OT (Q9/Q20/Q34)

3b. Vendor dependency could become a constraint for OT recovery objectives

- 76% of respondents claim to have recovery plans that require involvement from OT vendors or system integrators in case of a full SCADA/DCS/PLC system failure (Q40)
- Yet, written contractual information includes examples of 24–48-hour on-site response times and vendor-dependent resolution



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DISCUSSION

09 | 10 | 2026



DISCUSSION

Key takeaways for sector dialogue

- Overall resilience posture is respectable on paper, but the gap widens as we move towards OT
- Incident response lacks a common playbook across the sector
- Legacy infrastructure hinders OT prevention and detection - asset visibility, patch cadence, and monitoring all trail their IT equivalents
- OT recovery is not a learning curve of IT maturity — strong IT/B2B recovery capability may provide confidence in handling OT environments but the path to get there is largely unproven. Still,
 - How to test or improve testing??
- Confidence in maintaining gas supply through a prolonged OT outage is high – are rapid isolation/kill-switch arrangements and 100% manual compressor override capability enough?

Group

- Thoughts on stress tests
- Covering other critical sectors
- Your experience/lessons learned

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

 +30 693 651 3960

 ricardo.desousafigueiredo@enisa.europa.eu

 www.enisa.europa.eu

