Euro 7, Anti-tampering, and the Expanding Cybersecurity Landscape

Document Control

Title	**Euro 7, Antitampering, and the Expanding Cybersecurity Landscape**
Document Version	0.1
Date of Issue	
Document Owner	Liz James
Document Author	consultant
Classification	

Version History

VERSION	DATE	DESCRIPTION OF CHANGE
0.1	Initial Draft	
0.2		
0.3		
0.4		

Contents

Abstract 2

Introduction 2

Regulatory Foundations: Where Euro 7 Fits In 3

Anti-tampering in Euro 7: From Exhaust Pipes to Embedded Systems 3

Why Now? The Drivers Behind Euro 7's Anti-tampering Provisions 4

Euro 7 and the R155 Threat Catalogue 5

Lifecycle Reporting and Continuous Assurance 6

The Assurance Case Lens 7

Worked Examples: Where Euro 7 Meets the Road 8

- Example 1: Authenticated CAN for Heavy-Duty Vehicles 8
- Example 2: Software Update Artefact Integrity 9
- Example 3: Megawatt-Scale Charging as a Tampering Vector 9

Implications for Industry and Regulators 1010

- For Industry: From Parallel Tracks to Integrated Cases 1010
- For Regulators: From Gatekeepers to Ongoing Custodians 10
- The Shared Burden 1111

Conclusion 1111

Euro 7, Anti-tampering, and the Expanding Cybersecurity Landscape

Abstract

Euro 7 marks a turning point in European vehicle regulation. While widely framed as a final tightening of emissions limits, the regulation also introduces explicit requirements around anti-tampering and cybersecurity. This creates a new intersection between environmental compliance and the cybersecurity frameworks already established by UNECE R155 and R156, underpinned by ISO 21434 and ISO 24089.

What emerges is not just a new set of technical hurdles, but a different style of assurance. Emissions regulators are beginning to ask the kinds of questions cybersecurity regulators already pose: *How will you prevent manipulation? How will you prove resilience not just at approval, but across the lifecycle of the vehicle?* Certificates of Compliance for Cybersecurity Management Systems (CSMS) and Software Update Management Systems (SUMS), once viewed as parallel approvals, are now being pulled into emissions law as evidence that anti-tampering protections are real, systematic, and enduring.

This blog explores how Euro 7 extends the threat landscape beyond the scenarios captured in R155's Annex 5, how manufacturers must adapt their Threat Analysis and Risk Assessment (TARA) processes to capture emissions-specific cyber risks, and how regulators are shifting from snapshot testing toward continuous evidence. It argues that Euro 7 embeds cybersecurity into the very grammar of homologation, making structured assurance and lifecycle reporting indispensable to both compliance and trust.

Introduction

Euro 7 has been talked about for years as the last great tightening of European emissions law. Public debate has centred on tailpipe numbers, measurement methods, and the political trade-offs of keeping combustion alive into the 2030s. But hidden in the annexes is something more radical than a tweak to grams per kilometre. For the first time, emissions law itself speaks directly about tampering, not just in the old sense of removing a catalytic converter, but in the digital sense of manipulating the embedded systems that govern modern vehicles.

This shift matters because it signals a new alignment between the environmental regulators who write emissions rules and the cybersecurity regulators who have, until now, sat in their own silo. Where UNECE R155 and R156 introduced the obligation for manufacturers to operate a Cybersecurity Management System (CSMS) and a Software Update Management System (SUMS), Euro 7 now makes those obligations bite in an entirely different way: it ties them to the credibility of emissions compliance. In other words, a vulnerability in your update process is no longer just a "cyber risk." If that vulnerability allows a vehicle's calibration to be tampered with, it is now an emissions offence.

The practical consequence is that manufacturers cannot simply treat Euro 7 as another emissions curve to meet. They must revisit their threat analyses. R155's Annex 5 already contains a catalogue of cyberattack scenarios, but Euro 7 demands that these be re-read through the lens of anti-tampering. It asks a harder set of questions: which of these threats could plausibly be exploited to undermine emissions performance, durability testing, or on-road conformity checks? Which threats are new, unique to the linkage between software and emissions? And, most importantly, how will evidence of resilience be produced not just at type approval, but across the entire lifecycle of the vehicle?

For type approval authorities, this also represents a change of posture. They are no longer gatekeepers for a single test campaign. They are becoming custodians of continuous assurance. Certificates of Compliance for CSMS and

SUMS are only the starting point. Regulators will increasingly expect to see how those certified systems are applied to each new vehicle type, and how they will remain active over the life of that vehicle — in updates, in fleet monitoring, in incident response. The evidence package that once consisted of lab reports and measurement curves is being expanded to include update logs, triage records, and cybersecurity audit trails.

In this blog, I will explore what Euro 7 really means for automotive cybersecurity. I will compare its new anti-tampering requirements with the threat classes already captured in R155, highlighting both overlaps and gaps. I will draw on ISO 21434 and ISO 24089 to show how engineering processes can support compliance, and I will consider how lifecycle reporting and continuous evidence reshape what regulators ask for when new vehicle types are introduced. My aim is to frame Euro 7 not as a narrow tightening of environmental rules, but as part of a larger homologation assurance case — one that forces cybersecurity, software governance, and emissions compliance into the same conversation.

Regulatory Foundations: Where Euro 7 Fits In

To understand the novelty of Euro 7, it helps to set it against the backdrop of existing automotive cybersecurity regulation. Over the past five years, the UNECE framework has redefined how vehicles are approved. Two regulations in particular are now unavoidable for manufacturers seeking type approval in Europe: R155 on cybersecurity and R156 on software updates.

R155 requires every manufacturer to operate a CSMS. The idea is not that a car must be “proven unhackable” — an impossible claim — but that an organisation must demonstrate systematic control of cybersecurity risk. This means having processes to identify threats, analyse risks, treat vulnerabilities, and monitor vehicles over time. Approval is granted only when the regulator is satisfied that such a system exists and is being applied to the vehicle type in question.

R156 does the same for software. It mandates a SUMS, covering everything from update package signing to rollout governance. Where R155 addresses the organisation’s ability to secure its products, R156 ensures that security and functionality can be maintained across the vehicle’s operational life.

Both regulations hinge on a Certificate of Compliance (CoC). This is the regulator’s way of validating that the CSMS or SUMS is real and functioning. The certificate is granted at the organisational level, but every new vehicle type must then show that it is governed by those certified systems. Without a CoC, type approval is impossible.

Sitting behind both regulations are the engineering standards. ISO 21434 lays out the vocabulary and processes for cybersecurity engineering: threat analysis and risk assessment (TARA), risk treatment, validation, and verification. ISO 24089 does the same for software updates, codifying how update artefacts are built, verified, deployed, and traced. These standards do not carry legal force on their own, but they are the scaffolding regulators and industry lean on to demonstrate compliance.

Euro 7 enters this landscape from a different angle. Its primary mandate is environmental: emissions limits, durability requirements, on-road conformity testing. But by introducing anti-tampering provisions, it implicitly leans on the same machinery as R155 and R156. A manufacturer cannot show that a vehicle resists tampering unless it can also show that its CSMS and SUMS are alive, certified, and applied. The Certificate of Compliance becomes the hinge between emissions regulators and cybersecurity regulators.

This is the crux of the change. Where emissions compliance once relied on laboratory data and conformity checks, it now relies on cybersecurity evidence too. Regulators who once looked only at exhaust pipes must now scrutinise update logs, key management, and threat assessments. And manufacturers who once siloed “environment” and “cyber” teams must now present a single, joined-up assurance case.

Anti-tampering in Euro 7: From Exhaust Pipes to Embedded Systems

Anti-tampering in Euro 7: From Exhaust Pipes to Embedded Systems

Anti-tampering is not a new idea in European regulation. Euro 5 and Euro 6 both contained clauses designed to stop owners or workshops from removing after-treatment devices or disabling onboard diagnostics. These provisions were written with a physical world in mind: welded catalytic converters, sealed ECUs, and tamper-evident screws. The assumption was that the most likely manipulations would involve spanners, not scripts.

Euro 7 reframes that assumption. Vehicles are now software-defined, their emissions performance a function not just of pipes and filters but of calibration maps, update artefacts, and connected services. The regulation explicitly recognises that manipulation is no longer only physical but also digital. To tamper with a modern powertrain, you do not need to unbolt anything; you can reflash an ECU, spoof a sensor, or alter an update package.

The new regulation therefore places an obligation on manufacturers to ensure that emissions-critical functions cannot be bypassed, suppressed, or falsified through software or communications. This expands the anti-tampering lens into several categories:

- **Manipulation of calibration maps.** Performance tuners have long reflashed ECUs to improve power output, often at the cost of emissions. Euro 7 treats this as an emissions compliance breach, not just a warranty issue.
- **Sensor spoofing and injection.** Feeding false data to Nox, Lambda or particulate sensors could create the appearance of compliance while the engine pollutes. This is no longer just a technical curiosity — it is a regulatory offence.
- **OBD suppression.** Tools that disable diagnostic trouble codes or manipulate OBD messages undermine the credibility of in-service conformity checks. Euro 7 requires that these vectors be considered in assurance.
- **Update tampering.** If an attacker can install a rogue calibration via an insecure update path, emissions law is directly implicated. This ties anti-tampering explicitly to the SUMS requirements of R156 and ISO 24089.
- **Supply-chain manipulation.** Calibration data and emissions-related software flow through long chains of suppliers and toolchains. Euro 7 asks whether those links are themselves resistant to tampering.

What is striking is that most of these scenarios already exist in the **threat catalogue of UNECE R155**. Annex 5 lists classes of cyberattack including “unauthorised modification of vehicle software,” “manipulation of sensor data,” and “compromise of update processes.” The difference is that Euro 7 reclassifies these not only as cybersecurity risks but as **direct emissions risks**. The consequence of a successful attack is not only a potential data breach or denial of service, but a regulatory violation under emissions law.

For manufacturers, this changes the stakes. A TARA developed purely to satisfy R155 might identify ECU reflashing as a risk to safety or operations. Under Euro 7, that same risk must also be treated as a threat to emissions compliance, with a different set of regulatory consequences. The analysis cannot simply be recycled; it must be reinterpreted.

This is where the alignment with R156 and ISO 24089 becomes unavoidable. If emissions law requires assurance that update processes cannot be subverted, then the only defensible evidence is the artefacts generated by a SUMS: package signing, distribution logs, and audit trails. Likewise, ISO 21434 processes for threat analysis and risk assessment become essential in demonstrating that emissions-critical functions have been considered explicitly.

Euro 7 therefore stretches anti-tampering from a narrow mechanical clause into a broad digital assurance requirement. It does not replace R155 or R156 but cross-cuts them, forcing manufacturers and regulators alike to see that the same threats carry multiple consequences — for safety, for security, and now for emissions.

Why Now? The Drivers Behind Euro 7’s Anti-tampering Provisions

On paper, Euro 7 could have limited itself to setting new thresholds for particulates, NOx, and brake dust. Regulators could have trusted that cybersecurity would remain the territory of UNECE R155 and software updates the remit of R156. But they didn’t. They chose to embed explicit anti-tampering language in emissions law. Understanding why helps explain the stakes.

First, the legacy of Dieselgate. The Volkswagen emissions scandal revealed the fragility of trust in laboratory testing. Regulators saw how sophisticated software manipulation could undermine an entire regulatory regime, not through hardware tampering but through calibration logic designed to detect test conditions. The lesson was clear: if you don't address software manipulation explicitly, the credibility of emissions regulation itself collapses.

Second, the rise of the tuning and hacking ecosystem. What was once the domain of hobbyists with soldering irons is now an industry with online marketplaces, plug-and-play dongles, and downloadable reflashing tools. Consumers can purchase OBD devices that disable DPF warnings or re-map ECUs in minutes. For regulators, ignoring this parallel economy would be to concede compliance in practice, even if it is maintained in theory.

Third, the software-defined vehicle. Increasingly, emissions compliance is not a property of fixed hardware but of software configurations that change over time. Updates can alter torque maps, injection strategies, or even disable subsystems. That makes cybersecurity inseparable from environmental law. A secure SUMS is no longer just about consumer safety or data protection; it is about ensuring that emissions values remain meaningful after every update.

Fourth, the lifecycle lens. Older emissions regimes assumed compliance was proven at type approval and checked periodically in service. Euro 7 assumes the opposite: that threats will evolve, and that continuous evidence is required to demonstrate resilience. That shifts the regulator's posture from gatekeeper to ongoing auditor, and it demands a broader view of tampering than earlier regimes considered.

Finally, the political dimension. As the EU sets aggressive decarbonisation targets, public confidence in regulation is paramount. If consumers believe that vehicles can be easily manipulated — whether by manufacturers or by end users — trust in both the automotive sector and in European environmental policy erodes. Including anti-tampering explicitly in Euro 7 is as much about signalling as it is about enforcement: a way of demonstrating that lessons have been learned, that manipulation won't be tolerated, and that compliance is credible.

Taken together, these drivers explain why Euro 7 could not simply rely on R155 and R156. Cybersecurity regulations define the "how," but emissions regulators needed to anchor the "why." By making anti-tampering a matter of emissions law, Euro 7 ensures that digital manipulation is treated not as an abstract cyber risk, but as a direct regulatory violation with environmental and societal consequences.

Euro 7 and the R155 Threat Catalogue

UNECE R155 Annex 5 contains a list of example attack vectors — everything from "unauthorised modification of software" to "manipulation of sensor data" and "compromise of supply chain." This catalogue underpins most TARAs, offering a common vocabulary for threat identification.

Euro 7, however, reframes some of these threats and elevates their significance. A manipulation that under R155 might have been logged as a cybersecurity risk is, under Euro 7, also a direct emissions offence. That shift changes both the **consequence modelling** and the **evidence expected by regulators**.

Here's a comparative view, highlighting where Euro 7 extends beyond the baseline threat classes of R155:

Euro 7 Anti-tampering Concern	Closest R155 Annex 5 Example	Where Euro 7 Extends / Reframes	Example Attack Scenario	Evidence Regulators May Expect
Manipulation of emissions-related software (e.g. calibration reflashing to reduce AdBlue dosing)	"Unauthorised modification of vehicle software"	Euro 7 ties software integrity directly to emissions conformity and durability testing.	ECU remap disables SCR dosing while leaving OBD nominal.	SUMS signing records, calibration hash verification, secure boot logs.

Sensor spoofing or manipulation to falsify emissions readings	"Manipulation of sensor data"	Euro 7 demands explicit linkage to emissions compliance, not just functional safety.	Injecting CAN traffic mimicking NOx sensor readings.	Sensor authentication evidence, anomaly detection logs, conformity of production test traces.
Suppression or manipulation of OBD diagnostic codes	"Unauthorised access to vehicle OBD"	Already covered by R155, but Euro 7 elevates this to a core emissions compliance risk.	OBD dongle disables fault codes before inspection.	Access control measures, OBD protocol hardening, test bench demonstrations.
Tampering via insecure update process (rogue calibration installed)	"Compromise of update process"	Euro 7 requires emissions-specific risk treatment.	Side-loaded unsigned firmware that adjusts torque maps.	SUMS governance artefacts, signed package logs, update approval records.
Supply chain tampering of emissions-critical data	"Compromise of supply chain"	Euro 7 forces emissions-focused scrutiny of toolchains and suppliers.	Third-party calibration tool introduces altered lookup tables.	Supplier assurance records, SBOMs, chain-of-trust audit evidence.
Exploiting aftermarket tools to bypass emissions controls	"Exploitation of external interfaces"	Euro 7 reframes this as a direct emissions violation, even if safety impact is minimal.	Commercially available dongle disables DPF warnings.	Testing against known tools, records of blocking measures, fleet monitoring evidence.
Deliberate disabling of emissions-critical updates	"Denial of service against update services"	Under R155 this is availability; Euro 7 makes it an emissions conformity risk.	OTA update containing revised calibration never reaches vehicle.	Monitoring of update distribution, incident response records, proof of re-try policies.

What emerges from this comparison is not an entirely new threat universe, but a reframing of impact. Many of the attack surfaces were already familiar to cybersecurity engineers, but Euro 7 links them directly to the legitimacy of emissions regulation. For TARAs, this means threat consequence ratings must be revisited: what was once a "medium" cyber risk could now be a "high" regulatory risk, with legal and financial implications far beyond the IT domain.

Crucially, it also means that the evidence portfolio regulators will expect is different. A penetration test report may still demonstrate exploitability, but type approval authorities will want governance artefacts too: update signing logs, CoC references, conformity of production checks that show how tampering was considered in practice.

Lifecycle Reporting and Continuous Assurance

One of the most consequential changes Euro 7 introduces is the expectation that assurance does not end at type approval. Earlier emissions regimes were structured as a series of checkpoints: demonstrate compliance in the lab, prove conformity of production, and pass periodic in-service testing. Once the paperwork was stamped, attention drifted until the next regulatory milestone.

Cybersecurity has never fitted comfortably into this model, and Euro 7 brings that tension into the heart of emissions law. A calibration map can be secure on the day of type approval and vulnerable six months later if an exploit kit emerges in the aftermarket. A SUMS may distribute signed packages today, but a supply-chain compromise

tomorrow could inject malicious code into the toolchain. A CSMS might have met its obligations at audit, but if incident response falters during operation, resilience collapses.

That is why regulators are now shifting posture: from gatekeepers of a one-time event to **custodians of continuous evidence**. The Certificate of Compliance for CSMS and SUMS is only the beginning. For every new vehicle type, authorities are asking:

- How do you demonstrate that the certified organisational system is applied to this product?
- How will you continue to prove that anti-tampering protections remain effective as the vehicle evolves through software updates and field use?
- What evidence will you provide when conformity checks are performed years after approval?

This is where Euro 7 stretches the evidential burden. The regulator no longer wants a snapshot; they want a **trace over time**. That trace might include:

- **Update governance logs** showing how each calibration package was signed, validated, and rolled out.
- **Incident response artefacts** demonstrating how attempted tampering was detected, triaged, and mitigated.
- **Fleet monitoring outputs** that reveal whether emissions-critical protections are behaving as intended in real-world conditions.
- **Supplier assurance evidence** linking emissions-critical software back through the chain of custody.

For manufacturers, this changes the rhythm of assurance. Evidence can no longer be assembled hastily at approval gates. It must be generated as part of normal operations — a living assurance case rather than a static dossier.

The implications are stark for new vehicle types. An electric truck entering type approval cannot lean solely on design-time evidence. Regulators will expect to see that monitoring hooks, update governance, and incident response processes are already in place to ensure the vehicle remains compliant in year five as well as on day one. The CoC provides the organisational assurance, but Euro 7 ensures that this must be operationalised at the vehicle level, continuously.

In practice, this means type approval authorities will begin to act more like ongoing auditors than one-time examiners. They may request lifecycle artefacts during conformity of production checks, scrutinise incident response records, or require manufacturers to demonstrate how their CSMS has been applied to live fleet issues. Euro 7 pushes assurance from a point-in-time compliance exercise into a continuous regulatory relationship.

The Assurance Case Lens

One of the most powerful ways to make sense of Euro 7's new demands is through the language of assurance cases. Where prescriptive regulation asks you to check a box — install a component, run a test — Euro 7 asks something harder: demonstrate that your vehicle resists tampering that could compromise emissions performance. That is not a single requirement; it is a claim that must be unpacked, justified, and evidenced.

The **Claims–Arguments–Evidence (CAE)** model and its graphical cousin, **Goal Structuring Notation (GSN)**, are particularly well suited to this. They allow regulators and manufacturers alike to see not just the headline claim but how it is decomposed into sub-claims, what reasoning supports it, and what evidence anchors it.

Take a simplified fragment:

- **Claim:** The vehicle resists tampering that could undermine emissions compliance.
    - **Argument A:** The organisation operates a certified CSMS (R155) that systematically identifies and treats tampering threats.
    - **Argument B:** The organisation operates a certified SUMS (R156) that ensures only authentic, validated updates are applied.

- **Argument C:** Emissions-critical functions have been explicitly analysed in the TARA, and countermeasures implemented and verified.
- **Evidence:** Threat analyses, update signing records, conformity-of-production test results, intrusion detection logs, supplier assurance artefacts.

This structure matters because it links Euro 7 to the wider homologation picture. The Euro 7 fragment is not free-floating; it depends on the existence of a CSMS and SUMS, evidenced by Certificates of Compliance. It also depends on ISO 21434 processes for threat analysis and ISO 24089 practices for update integrity. The result is a **joined-up case** that regulators can interrogate rather than a pile of disconnected documents.

It also helps avoid the **"pentest trap."** In cybersecurity, there is a temptation to substitute a single activity — a penetration test and a fuzzing campaign — for an assurance case. But Euro 7 requires more. A pen test showing an ECU could not be reflashed without credentials is valuable evidence, but only if it is embedded in a broader argument: that the SUMS enforces credentialing systematically, that the CSMS triages any findings into the risk process, and that evidence is retained to prove this over time. Without that structure, evidence is brittle; with it, evidence becomes living assurance.

For regulators, this style of reasoning is not abstract. It directly changes how they review submissions. Instead of reading narrative reports, they can trace dependencies: *How does this update log connect back to your SUMS? How does your SUMS connect back to your CoC? How does that CoC underpin the Euro 7 claim?* The assurance case makes these linkages explicit, and it allows gaps to be spotted quickly — for example, if a threat class from Annex 5 is absent from the Euro 7 fragment.

For manufacturers, building assurance fragments also supports reuse. A fragment created for "tampering via insecure update" in Euro 7 can also strengthen the R156 case. A fragment created for "sensor spoofing" can support both R155 (safety/security) and Euro 7 (emissions compliance). Instead of reinventing the wheel for each regulation, fragments can be assembled into a coherent whole.

Ultimately, the assurance case lens reframes Euro 7 not as a bolt-on obligation but as another piece of a wider puzzle. By articulating claims, arguments, and evidence explicitly, manufacturers can show that emissions integrity, cybersecurity, and software governance are not three separate silos but one integrated assurance story.

Worked Examples: Where Euro 7 Meets the Road

Abstract discussions of "anti-tampering" risk becoming vague. To see what Euro 7 really demands, it helps to look at concrete scenarios — places where emissions compliance, cybersecurity, and update governance intersect.

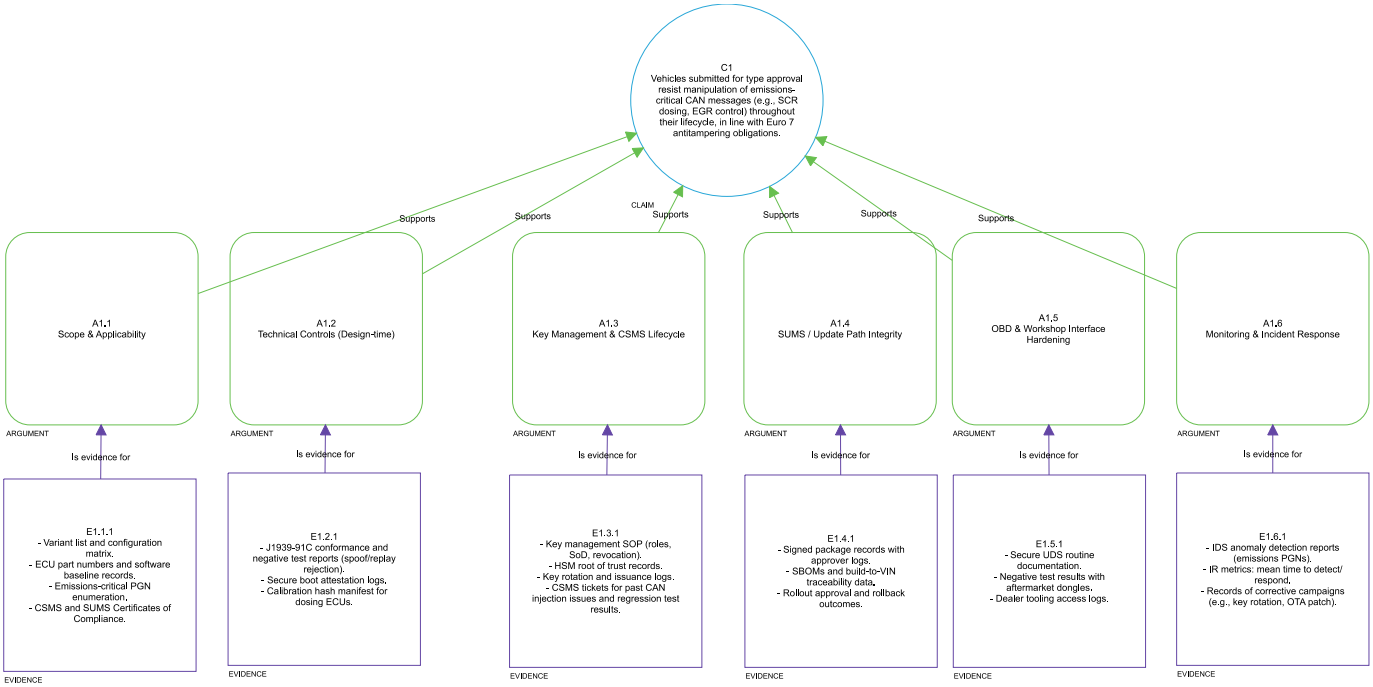
Example 1: Authenticated CAN for Heavy-Duty Vehicles

Heavy-duty trucks rely on J1939 communications for emissions-critical functions like SCR dosing and EGR control. Under R155, threats such as CAN injection attacks are already in scope. But Euro 7 reframes these as direct emissions compliance risks.

Consider a rogue tool injecting spoofed CAN messages to disable AdBlue dosing. Under R155, this is a cybersecurity breach. Under Euro 7, it is also a manipulation that undermines emissions durability testing. Evidence regulators will expect may therefore include:

- Implementation of authenticated CAN (J1939-91C).
- Cryptographic key management records showing how credentials are provisioned and rotated.
- Test artefacts demonstrating that spoofed messages cannot bypass dosing logic.
- Triage records showing how any vulnerabilities discovered were fed into the CSMS.

The assurance case ties this evidence together, showing that emissions-critical communication cannot be manipulated without detection.



Example 2: Software Update Artefact Integrity

R156 and ISO 24089 already require secure update management. Euro 7 pushes this further by treating insecure updates as potential emissions violations.

Imagine a scenario where an aftermarket workshop attempts to side-load a calibration that enriches fuel maps but suppresses OBD faults. To defend against this, the manufacturer must show that:

- All update packages are signed and validated against a trusted root.
- Distribution logs record which vehicles received which packages and when.
- Update failures or anomalies are detected and trigger incident response.

Here the regulator's lens is not just cybersecurity but emissions compliance. A rogue package is no longer "just" a cyber risk — it is a breach of Euro 7. The evidence portfolio therefore spans both domains, linking SUMS artefacts directly to emissions obligations.

Example 3: Megawatt-Scale Charging as a Tampering Vector

As heavy-duty EVs enter service, megawatt charging systems create new attack surfaces. A compromised EVSE could attempt to disrupt charging logic in ways that indirectly impact thermal management or battery operation, with knock-on effects for emissions-equivalent measures like energy efficiency or brake dust profiles.

Under R155, this might be considered a safety or availability issue. Euro 7 reframes it as a potential manipulation of regulated parameters. Regulators may ask:

- How is charging communication secured (e.g. ISO 15118-20 with TLS and certificate management)?
- How are emissions-related parameters (such as efficiency metrics) protected against manipulation in charging events?
- What fleet monitoring evidence shows resilience against adversarial charging stations?

The assurance case here links external infrastructure threats to emissions compliance, showing how anti-tampering analysis extends beyond the vehicle into its ecosystem.

Example 4: Sensor Spoofing of NOx Readings

In-lab emissions testing depends heavily on sensor accuracy. A malicious actor could inject false NOx data to pass tests while the vehicle emits above the limit. Under R155, this is captured under "manipulation of sensor data." Euro 7 elevates it: such spoofing now directly undermines emissions law.

Evidence might include:

- Sensor authentication mechanisms (e.g. challenge–response between sensor and ECU).
- Intrusion detection logs capturing anomalous NOx readings.
- Conformity-of-production checks verifying sensor integrity.

In the assurance case, the argument is simple: NOx data cannot be falsified without detection, and evidence shows countermeasures working in practice.

Implications for Industry and Regulators

Euro 7's anti-tampering provisions do not land in a vacuum. They reshape expectations for how manufacturers prepare, how regulators review, and how both sides maintain trust in type approval.

For Industry: From Parallel Tracks to Integrated Cases

Manufacturers have long treated emissions compliance, cybersecurity, and software governance as three separate regulatory streams. Euro 7 removes that luxury. A single vulnerability — say, a reflashing tool bypassing OBD protections — can now ripple across all three domains: it is a cybersecurity weakness (R155), a governance failure (R156/ISO 24089), and an emissions violation (Euro 7).

The implication is that **TARAs must be extended**. It is no longer enough to show that threats are identified and mitigated in safety or security terms; each threat must also be evaluated for its potential impact on emissions compliance. That requires closer collaboration between calibration engineers, cybersecurity teams, and regulatory affairs.

Operationally, evidence portfolios must also expand. Logs, signing records, triage documents, supplier audits — these artefacts must be collected systematically, not just for internal assurance but with the expectation that regulators will ask to see them. Building them into the CSMS and SUMS from the start is essential to avoid unmanageable "assurance debt" later.

For Regulators: From Gatekeepers to Ongoing Custodians

For type-approval authorities, Euro 7 demands a different posture. The familiar model of witnessing tests and reviewing lab results is no longer sufficient. Regulators must now interrogate structured assurance cases, Certificates of Compliance, and lifecycle evidence streams.

This implies three shifts in practice:

- **From snapshot to longitudinal review.** Regulators should expect to review logs, incident records, and update artefacts across a vehicle's life rather than only at approval.
- **From component to system view.** Instead of verifying whether a single sensor meets calibration standards, regulators must ask how sensor data integrity is maintained across the whole system, including interfaces and supply chains.
- **From observation to reasoning.** The real assurance value lies not in watching a test run but in understanding how a manufacturer reasons about threats, applies its CSMS/SUMS, and evidences its processes.

This also means regulators themselves may need new capabilities. If structured CAE/GSN cases are adopted more widely—as we advocate—they could provide a consistent way to organise the disparate material that comprises a compliance case. The challenge for regulators will be less about reading individual pieces of evidence and more about evaluating that evidence within the context of the OEM's argument: does the reasoning link controls to risks,

are assumptions explicit, and does the evidence actually support the claimed conclusions. Interpreting cybersecurity evidence and assessing supplier governance in this argumentative, systems-level way are skills emissions-focused authorities, or regulators traditionally oriented around inspections and procedural checks, may not yet possess. Euro 7 therefore implies a need to invest in regulator expertise as well as in manufacturer compliance.

The Shared Burden

Perhaps the most important implication is that Euro 7 creates a **shared burden of assurance**. Manufacturers cannot simply produce emissions test data and regulators cannot simply witness it. Both sides must engage with living assurance cases, built on structured reasoning and continuously updated evidence.

Done well, this shift can build confidence: confidence that vehicles remain compliant over time, confidence that manipulation is deterred, and confidence that environmental goals are not quietly undermined by technical shortcuts. Done poorly, it risks producing compliance theatre: glossy narratives unsupported by real evidence, or fragmented TARAs that overlook emissions-specific risks.

Euro 7 therefore sets the stage for a new era of homologation, one where cybersecurity and emissions compliance are no longer parallel obligations but intertwined threads of a single assurance story.

Conclusion

Euro 7 is often described as the last tightening of Europe's emissions regime. In practice it is something more significant: a bridge between environmental law and cybersecurity regulation. By embedding anti-tampering obligations, Euro 7 makes it impossible to treat emissions and cyber as separate silos. The same threats UNECE R155 catalogues as cybersecurity risks now carry direct regulatory weight under emissions law.

For manufacturers, this demands a rethinking of assurance practice. Threat analyses must explicitly consider emissions impacts; Certificates of Compliance for CSMS and SUMS must be applied and demonstrated at the vehicle level; and evidence must be generated and curated continuously rather than assembled hastily at approval gates. Anti-tampering can no longer be an afterthought it must be designed into updates, monitoring, and incident response.

For regulators, the challenge is equally stark. Type-approval authorities are being asked to move from witnessing emissions tests to interrogating living assurance cases. They will need new skills, processes, and capacity to review logs, triage records, audit suppliers, and evaluate both tacit and explicit assurance artefacts. Many manufacturers will initially present tacit cases assembled from piles of ISO/SAE 21434 work products and project outputs; others may adopt more explicit, structured CAE/GSN cases that link argument, evidence, and assumptions clearly. The regulatory task is less about reading individual pieces of evidence and more about judging that evidence inside the OEM's argument: are assumptions explicit, do controls map to identified risks, and does the evidence actually support the claimed conclusions. Euro 7 therefore requires investment in regulator expertise as well as in manufacturer compliance.

For the wider system, Euro 7 signals a deeper truth: in software-defined vehicles there is no clean boundary between emissions, safety, and security. They are facets of the same assurance problem — ensuring that what a vehicle does in the real world matches what society has approved in principle. That requires structured reasoning, reusable assurance fragments, and acceptance that compliance is dynamic, evolving with every update and every threat.

If Euro 7 succeeds, it will be remembered not for the particulate numbers in its annexes but for making cybersecurity part of the grammar of homologation — the moment emissions law and cyber law stopped running in parallel and became a single assurance case. Assurance cannot be static. Anti-tampering is not a one-off test, and cybersecurity is not a dossier filed at type approval. Both demand evolving reasoning, refreshed evidence, and confidence built through scrutiny.

Assurance cases thrive where they are challenged, reviewed, and refined. Peer review is not optional — it is how claims gain credibility, arguments are stress-tested, and evidence is judged sufficient by regulators and industry alike. As Euro 7 embeds cybersecurity into homologation, the industry must respond with assurance practices that are transparent, collaborative, and resilient.

If you would like to discuss these ideas further, share perspectives on Euro 7, or explore how structured assurance cases — tacit or explicit — can be developed and reviewed in practice, please reach out: liz.james@nccgroup.com

Together we can ensure the shift from static compliance to living assurance delivers what regulators, manufacturers, and society need most: trust in the integrity of the vehicles we put on the road.