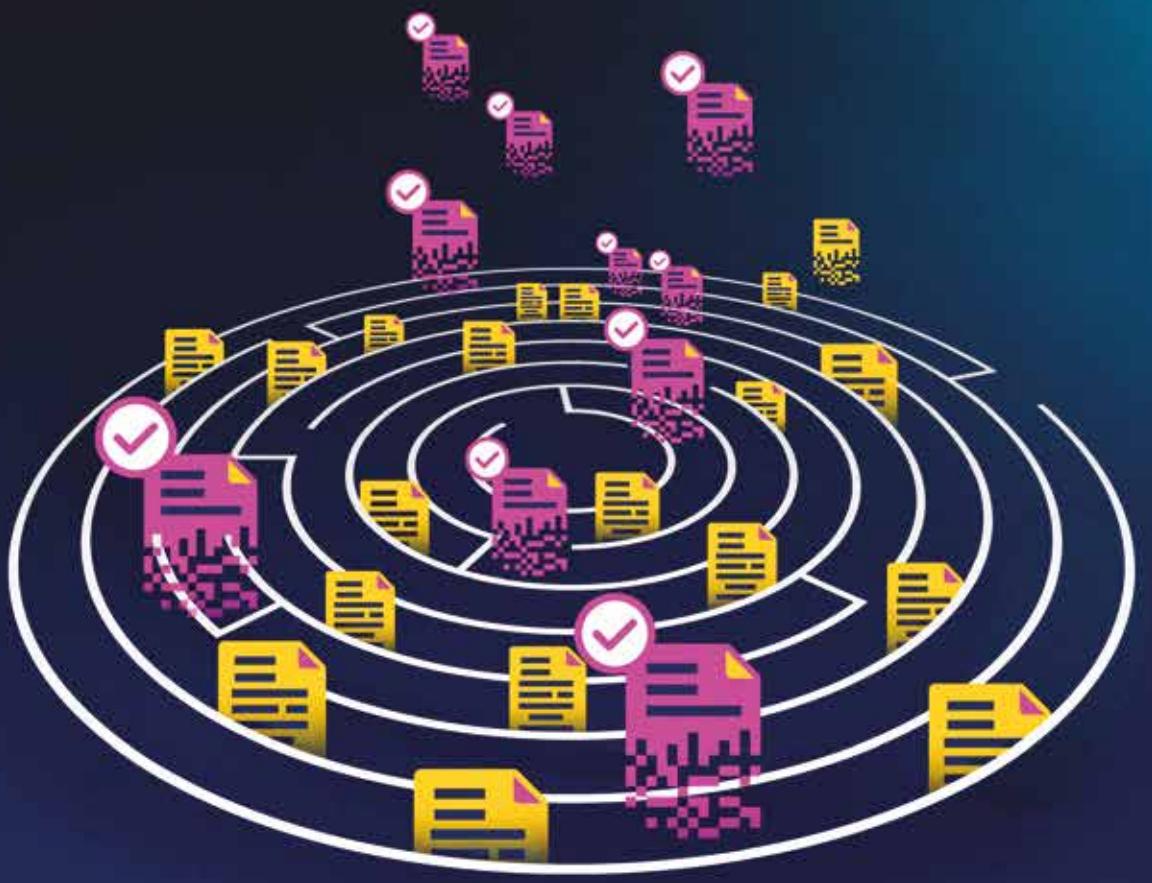

REDEFINING TRACEABILITY

Mario Pierobon reports on how emerging regulations are redefining acceptable practice in component traceability

Component traceability in aviation has long been defined by the presence of correct certificates and records.

Regulatory authorities are now redefining acceptable practice, shifting focus from document repositories to data integrity and continuous chain-of-custody verification.

This evolution is exposing fundamental limitations in legacy systems and revealing persistent vulnerabilities across the supply chain, particularly in the detection of suspected unapproved parts.

What is being witnessed is a clear shift in regulatory expectations, not so much a radical change in the standards themselves, but rather a shift in how those standards are interpreted and applied, according to Gary Jones, senior product manager at Veryon.

"Historically, traceability was often assessed based on the presence of the correct documentation and its consistency," explains Jones. "Today, regulators place much greater emphasis on the integrity and continuity of underlying documentation.

"In practice, this means being able to demonstrate a consistent chain of custody throughout the component's lifecycle, without unexplained gaps, and with information that can be cross-referenced with other sources, if necessary.

"It is important to note that regulators are not universally mandating fully digital, end-to-end traceability systems. However, through guidance, oversight and enforcement, particularly in the context of suspected unapproved parts (SUP), they are clearly indicating the direction to follow, and that direction is becoming increasingly explicit."

Regulatory frameworks are redefining acceptable component traceability, shifting focus from documentation completeness to data integrity, according to Jason Cordoba, chief executive of CordobaQ.

"Historically, compliance meant maintaining comprehensive documentation, such as FAA 8130-3 or EASA Form 1 certificates," says Cordoba. "We observe that regulators increasingly expect verifiable end-to-end traceability, including a continuous chain of custody and validation of data authenticity.

"This shift is exposing the shortcomings of many ERP systems, which remain document-centric and unable to structure, validate or verify traceability data. As a result, they

"TRACEABILITY COMPLIANCE NOW REQUIRES DEMONSTRABLE DATA INTEGRITY, NOT MERELY DOCUMENT ARCHIVES"

struggle to detect inconsistencies, gaps in production history, or duplicate component identities across transactions."

Karmendra Jaisi, senior engineer for technical services at EirTrade Aviation, points out that aircraft components must always have a clear and traceable history.

"Industry-wide, common practice is that non-life-limited-parts (LLPs) require minimum traceability records back to the last operator, or to the approved shop (Part 145)," explains Jaisi. "LLPs, on the other hand, require full traceability from the source and commercial documentation, such as sales invoices, from the manufacturer to the current owner.

"At EirTrade Aviation, we manually verify documentation based on our internal requirements, as well as regulatory and commercial requirements. These processes identify any fraudulent documents or certificates, ensuring that components are purchased and sold only from authorised sources."

In Europe, for example, there is a steady shift toward formal recognition of digital documents, more stringent traceability requirements, and the introduction of data integrity and information security frameworks, such as Part-IS, Jones affirms.

"At the same time, regulatory attention is growing on the use of automated systems and analytics, particularly when they influence airworthiness decisions," he says. "Overall, these developments point to a trend toward a more data-centric regulatory model, where traceability is not limited to the mere presence of documents, but involves demonstrating that the underlying data is complete, secure and reliable."

This shift in approach is exposing some fundamental limitations of existing software platforms, according to Jones. "Many systems currently in use were designed primarily as document repositories rather than validation tools. They store certificates, work orders and release documentation, but do not necessarily ensure their consistency with other parts or verify their authenticity.

"Data remains fragmented among OEMs, MROs, distributors and operators, and much of it is still exchanged in unstructured documents such as PDFs.

"Standards exist (e.g. ATA Spec 2000), but their adoption is inconsistent throughout the supply chain, creating ambiguity in how components and serial numbers are recorded and interpreted. This lack of consistency creates opportunities for error and, in some cases, abuse," says Jones.

Audits highlight recurring risks such as including falsified certificates and used components falsely presented as functional, affirms Cordoba. "In many cases, these issues are hidden by complex supply chains and are only identified through deeper data analysis," he says.

"The direction is now clear: acceptable traceability is no longer defined by the presence of documents, but rather by the ability to demonstrate their authenticity and continuity. This is driving the need for more advanced, data-driven platforms capable of validation, anomaly detection and transparency across different systems."

Patterns are relatively consistent regarding enforcement trends, Jones points out. He says: "The most common problem remains falsified or altered release certificates (documents that appear valid but are not). At the same time, regulators are increasingly identifying what might be called 'reuse' or 'recycling' of documentation, where legitimate documents are applied to components for which they were never intended.

"Another recurring theme in audit findings is incomplete traceability that is not immediately apparent such as a lack of ownership history, undocumented maintenance, or gaps during storage or transfer. These issues are often identified only when records are examined as a whole, rather than document by document."

There are also simpler cases of misrepresentation, such as used components presented as new or inconsistencies between serial numbers and supporting documentation, affirms Jones. "These cases typically fall under the broader category of SUPs, which remains a key focus area for regulators and the industry in general. Therefore, while the regulatory framework itself has not been radically rewritten, expectations, and increasingly the future regulatory framework, are shifting toward demonstrably continuous, digitally robust and independently verifiable traceability. The challenge is that much of the existing infrastructure was never designed with this level of control in mind," he says.

The regulatory trajectory is evident: traceability compliance now requires demonstrable data integrity, not merely document archives. Legacy ERP systems, designed as repositories rather than validation platforms, struggle to meet emerging expectations for continuous verification and anomaly detection.

As enforcement intensifies around falsified certificates, documentation recycling and incomplete custody chains, operators and MROs face mounting pressure to transition toward data-centric platforms capable of cross-referencing, authenticating and validating component histories across fragmented supply chains.

The infrastructure challenge is substantial – much of the existing framework was never architected for this level of scrutiny. ●

Illustration Phil Couzens