SOFTWARE'S MODERN MOVEMENT

Machine learning and cybersecurity are the watchwords of today's systems, but do the two need to be mutually exclusive?

"They always say time changes things, but you actually have to change them yourself," as pop artist Andy Warhol once said. He might have been musing on the essence of personal responsibility and action, but the same could be said of the march towards digitalisation in the airline industry.

While the work behind the scenes to make the latest software secure without compromising its effectiveness is vast, improvements in the world of artificial intelligence and machine learning are driving the industry towards being both more efficient and more effective.

"We're just getting started with what IT and AI can do for regional aviation and aviation MRO," says Kris Volrath, SVP of aviation maintenance software publisher Veryon. "Right now, a lot of maintenance operations still rely on manual processes, rigid schedules and fragmented data – but that's changing fast."

Volrath is of the opinion that AI can make sense of 'big data' where traditional data management programmes have struggled. "One of the biggest shifts we're seeing is AI helping airlines move from scheduled maintenance to predictive maintenance," he explains.

"Instead of fixing something because a schedule says it's time, operators can use AI to analyse flight data, defect logs and maintenance history to predict when a part will fail. That means fewer unnecessary maintenance checks, less downtime and lower costs."

John Stone, VP product management at Ultramain Systems is also of the opinion that machine learning-type systems can offer efficiency, accuracy and operational visibility, although he does add a caveat: "While advancements in automation are making strides, not enough is being achieved in optimisation.

"With the vast amount of data now available in MRO environments, there is a critical need for solutions that go beyond automation – guiding users toward the best possible outcomes in any given situation."

▶ Veryon software utilises AI technology to diagnosis issues more efficiently

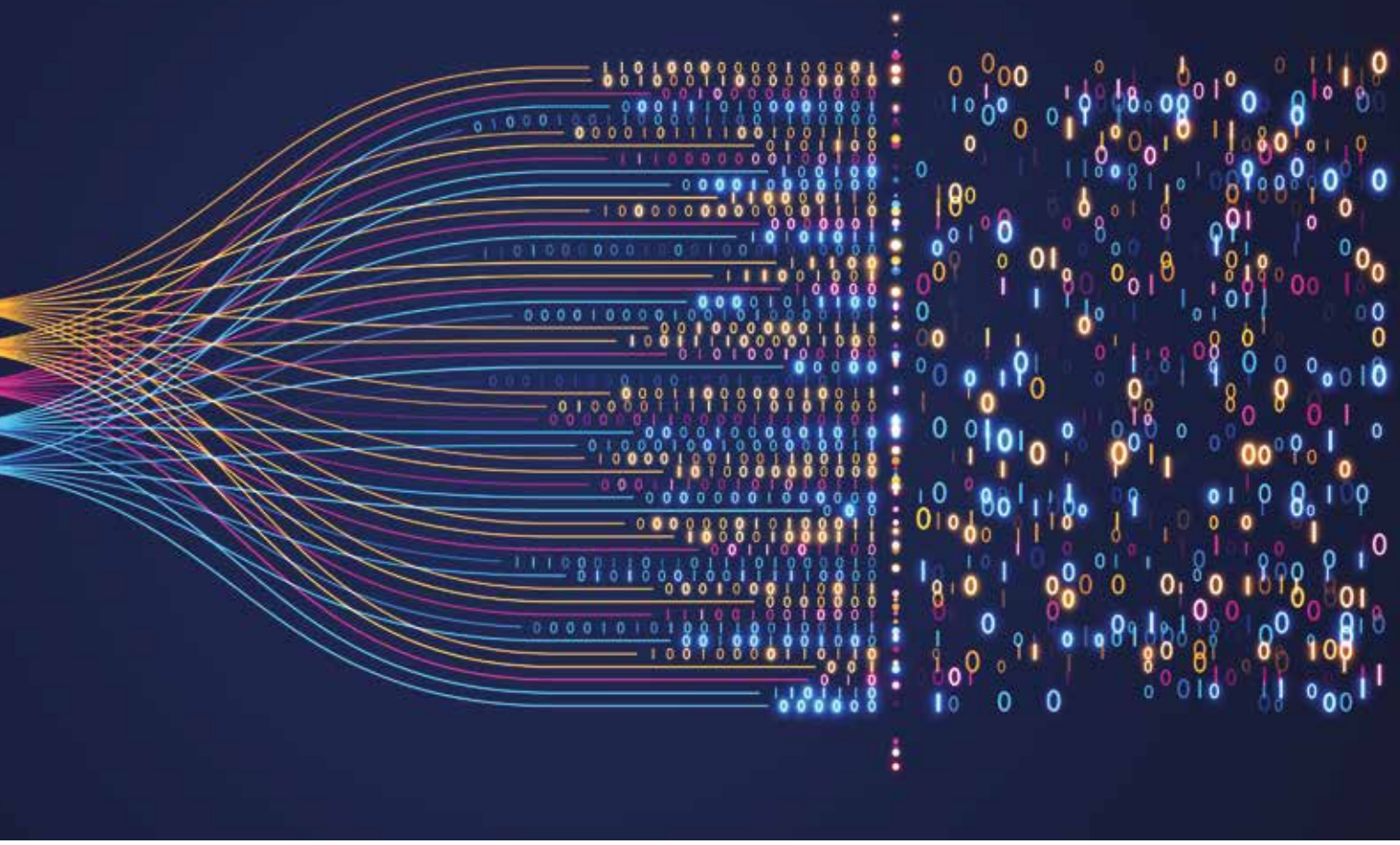
Automation and data

Automation is another word that comes up a lot when talking about modern systems. "However,' says Stone, "true efficiency is not just about automation, it's about making data actionable."

He continues: "Ultramain Scenes are intuitive, data-driven visualisations that present complex MRO data in an actionable, user-friendly interface. By leveraging real-time operational insights, they provide a path through tasks such as hangar planning, check scheduling, aircraft conversions, production workflows and warehouse picking.

"Rather than just displaying data, our software actively guides users toward the most efficient decision at every stage of the maintenance process."

Veryon's Volrath also explains that actionable data is more important than just having the ability to process stacks of information. According to him, troubleshooting is one of the biggest 'pain points' in MRO.



◀ (Far left) Ultramain Systems offer cloud hosting and managed services (Left) Veryon's Kris Volrath

"Right now, when a technician is trying to diagnose a problem, they might have to sift through pages of manuals past maintenance records, and even rely on trial and error. With an AI-powered tool like Veryon Diagnostics, we are building towards a future where AI can automatically identify patterns in maintenance data and historical defect trends that human engineers may miss.

"By providing early warnings, pinpointing root causes, assessing parts availability, and reducing AOG time, maintenance teams can address the correct problem and improve asset utilization, reduce delays, and minimize operational disruptions by improving first-time fix rates."

Critical cybersecurity

For reasons that we don't need to go into now, the need to keep data out of the wrong hands has never been so pressing.

Ultramain Systems' John Stone is clear on the need for enhanced security: "Cybersecurity in aviation maintenance is a mission-critical priority that ensures operational resilience, regulatory compliance, and passenger safety.

"With the aviation industry increasingly reliant on interconnected digital ecosystems, we take a multi-layered approach to cybersecurity, focusing on three primary tracks: infrastructure security, data security and software security.

"Each of these areas plays a crucial role in safeguarding aviation IT systems from cyber threats, with natural overlaps that strengthen overall protection. Data security ensures the confidentiality, integrity and availability of flight logs, maintenance records and operational data."

Stone continues: "At Ultramain Systems, we protect this data with encryption both in transit and at rest, ensuring secure transmission and storage. Role-based access controls, multi-factor authentication and strict data governance policies further safeguard sensitive information, allowing only authorised personnel to access or modify critical data. By maintaining robust encryption standards and access controls, we help ensure both regulatory compliance and operational security.

"Infrastructure security protects the network architecture, cloud environments and on-premises systems that support aviation maintenance. This includes firewalls, endpoint security and access controls to prevent cyber intrusions. At Ultramain Systems, we offer cloud hosting and managed services, allowing customers to leverage our secure infrastructure and compliance-driven approach while focusing on operations."

Kris Volrath concurs with the imperative to build robust cybersecurity measures into each product.

"Cybersecurity isn't a one-time fix – it's an ongoing process. As threats evolve, we continuously test and update our systems, work closely with industry experts and refine our practices. At the end of the day, aviation IT is all about trust. Operators need to know their data is safe so they can focus on keeping aircraft flying, and that's exactly what we're committed to delivering," he explains, adding that a challenge for his firm, and others like it, is the ability to balance customer data accessibility while ensuring algorithms can continuously learn and improve to benefit all.

"Airlines, OEMs and MROs need immediate access to maintenance logs and parts data within our products," Volrath says. "Yet, that information must be shielded from both cyber threats and not co-mingled across customers. We've addressed this with our multi-tenant strategy combined with anonymised datasets for benchmarks. This approach allows us to rapidly be training algorithms and AI models but also ensure our customer's data is always protected."

To call back to Warhol, the artist once mused on the nature of work that "the machinery is always working, even when you sleep". The same message can be applied to today's systems, where the user needs not worry about the big number-crunching going on in the background. That bodes well for the future efficiency of our business.

"CYBERSECURITY IS AN ONGOING PROCESS. AS THREATS EVOLVE, WE CONTINUOUSLY TEST AND UPDATE OUR SYSTEMS"