[Big Data, analytics and the Aircraft Internet-of-Things to revolutionize the operational efficiency and safety of Aircrafts]

The Indian Air Force Sukhoi-30 fighter jet was on a routine training mission, when it lost radar and radio contact with the controlling station near Arunachal Pradesh's Doulasang area, an area adjoining China. Blackbox or flight data recorder has been recovered by the Search team. IAF has ordered a court of enquiry for the crash. Last year, a Sukhoi-30MKI crashed near Nagaon town of Assam during a routine sortie. While the two pilots ejected safely, some locals suffered splinter injuries from the crash. The IAF's Sukhoi-30 fleet has been plagued by engine troubles and poor serviceability.

The international analysts based in Russia and the United States, have warned that the loss of an advanced and mechanically certified as safe, Sukhoi 30 fighter aircraft, close to the border with China may be the result of "cyber-interference with the onboard computers" in the cockpit. This may explain why even the pilots may have found it difficult to activate safety ejection mechanisms, once it became obvious that the aircraft was in serious trouble, as such mechanisms too could have been crippled by computer malfunctions induced from an outside source.

They point to the apparent loss of five Army vehicles, "due (according to the authorities) to a misfired mortar strike" in the same zone, saying that a single mortar round would not have enough firepower to take out such a large number of vehicles. They add that the possibilities are that the damage may have been caused by a larger projectile guided by electronic systems that may have been interfered with during flight. Given the range and complexity of cyber interference, the source of the attack could have been from thousands of kilometres or from only a few hundred metres away. These analysts warn that although India spends over Rs 200,000 crore on defence through the armed forces and another Rs 100,000 crore on security via police units, hardly Rs 4,700 crore gets spent on cyber capability.

Given the right sensors and software, IoT technology could detect an anomaly in a jet engine or its associated hardware, software or systems. This could, in theory, prevent accidents. Using emerging technology like IoT thousands of sensors can be embedded in each aircraft which transmit real time location data of aircraft, real-time performance and health of their engines and avionics to the maintenance personnel on the ground, who in turn use big data and real time analytics to deal with potential problems and also aid in search and rescue.

The Russian Foundation for Advanced Research Projects has come up with an idea of equipping Russian airliners, including MC-21 with what it briefly described as a “nervous system” for monitoring the technical condition of all of the airframe’s components and parts, project chief Dmitry Uspensky told TASS.

IoT in Airline sector

By 2025, it is predicted that there can be as many as 100 billion connected IoT devices or network of everyday objects as well as sensors that will be infused with intelligence and computing capability. These devices shall comprise of personal devices such as smart watches, digital glasses and fitness monitoring products, food items, home appliances, plant control systems, equipment monitoring and maintenance sensors and industrial robots.

For the airline sector, IoT offers multiple opportunities to improve operational efficiency and offer increased personalisation to passengers. Among airlines that have started experimenting with IoT, there are projects to improve passenger experience, baggage handling, tracking pets in transit, equipment monitoring, and generating fuel efficiencies. Real time location data of aircraft that impact a host of actions ranging from Advertising bill boards to flight information dashboards to deciding on optimized routes.

Tim Graham, technology innovation and development manager at Virgin Atlantic, suggests numerous possibilities: “On the ground, it could be mounted displays, mobile or wearable devices combined with sensors… to either help passengers navigate their surroundings, identify themselves at check-in, lounge or boarding areas or track objects such as baggage and cargo.”

He adds. “In the air, it could be intelligent aircraft cabins that have sensors built in to seats that could monitor passengers’ tiredness, temperature or hydration levels to automatically change the cabin environment or alert crew to take a specific action.”

Another project, rolled out in 2014, is the collection of data generated by the aircraft and its systems into a fuel management dashboard that also integrates operational, weather, trajectory correction, navigation, and terrain data. This tool has allowed AirAsia to optimise climb profiles, plan taxi and contingency fuel needs, and minimise the use of auxiliary power units.

IoT is tipped to revolutionize the aerospace industry in many ways. It is transforming day-to-day tasks in aviation ranging from assembly and manufacture to maintenance and safety, including tracking an aircraft’s location. Integrating IoT in aviation helps to tackle complex situations by adopting new trends like embedded sensors in engines, device monitors, data storage and information technology advances. Its device integration requires the support of hundreds of touchpoints and notifications, alerts, and customized application development. A lot of this data already resides in public, private or hybrid clouds. But it has to be easily accessible by aviation companies for commercial use. Recently, the trend is shifting to aerospace companies having the ability to manage connected devices from a single interface.

However, today’s use of IoT technologies for greater efficiency is scratching the surface compared with what could be achieved in the future. “IoT applications could improve overall fuel cost (not just the consumption) taking into account energy prices, when/where to refuel, optimal flight and taxi paths as well as when/how much to hedge for the fuel,” says GE’s Bartlett. “Beyond that, IoT applications could look at network optimisation, in particular the irregular operations recovery options as they continue to try to maximise the utilisation of their fleet while keeping a robust schedule.”

Russian planes to be equipped with ‘nervous system’ for monitoring airframe flaws

The Russian Foundation for Advanced Research Projects has come up with an idea of equipping Russian airliners, including MC-21 with what it briefly described as a “nervous system” for monitoring the technical condition of all of the airframe’s components and parts, project chief Dmitry Uspensky told TASS.

Using a system of early warning of likely flaws and faults on the MC-21 plane is not only possible but very desirable. From the standpoint of compatibility it is a soluble problem. Such a technology of continuous monitoring of the plane’s condition will be very helpful in creating a system for prompt, online maintenance depending on the aircraft’s actual condition. Our new generation plane will appear on the market in a very different economic situation,” Uspensky said.

The composite materials of which the planes are made will incorporate optical fibers sensitive to mechanical impact. The fibers will constitute an integrated network.

“Data showing the condition of the given component will be transmitted by a laser beam travelling within the optical fiber to the system’s ‘brain’ – the onboard computer. As a result, information about the technical condition of certain critically important parts, units and elements of the plane will be promptly available to the pilot and ground services,” Uspensky said.
He pointed out such a feature was of key importance to ensuring flight safety.

“The relevance and authenticity of information about the plane’s technical condition is crucial to timely adjustment and repairs of potentially faulty components. This will save lives,” he said. “The nervous system the Foundation is working on is unparalleled,” Uspensky pointed out. “Nobody has anything similar to what we are about to create.

Currently most planes are equipped with systems of warning the pilot about the dangerous condition of engines. The world’s leading manufacturers of air turbines equip them with automatic systems of gathering information about their current condition and transmitting them to the ground services. But all of such systems monitor the operation of only one unit of the plane, albeit a key one.

“The Russian system is meant for enhancing the effectiveness of maintenance of the plane’s airframe: the wings, tail, fuselage, etc., in other words, the basic elements of the plane’s structure crucial to flight safety,” Uspensky added.

IoT Technologies

The technologies that enable IoT are not in themselves complicated: the latest version of the internet communications protocol, IPv6, which allows for trillions of nodes (or IP addresses) on the internet and wireless proximity-detecting technologies, such as Bluetooth low energy (BLE) beacons, radio frequency identification tags and near-field communications.

As Peters notes, much of the innovation is focused on enabling IoT devices to communicate. Google recently announced Brillo, an underlying operating system for IoT devices, and Weave, a cross-platform common language that will let devices communicate with each other locally and via the cloud.

New aircraft models like Dreamliners for instance come pre-designed with IP enabled avionics systems that permit real time data to be transmitted to the cockpit and to operations centers on the ground on flying conditions and discrepancies observed during the flight.

Chief information officers’ focus, he suggests, should be on getting the architecture right for IoT. “A key component of the IoT framework will be the middleware platform, which will manage the enormous amount of messages generated at speed.

Also, the IoT value will only come alive if smart machine learning algorithms are able to garner insight from the data collected from the sensors and suggest actions in real time. Such architectural components will be crucial to making IoT happen and driving true business value out of the implementations.”

Aerospace IoT shall generate Huge Data

Military and commercial airline operators face a significant increase in data as they embrace the Internet of Things for fleets of highly connected aircraft capable of creating half a terabyte of data per flight per day. Loadable software airplane parts, aircraft health maintenance data, performance data from e systems and components, data used to track cargo and baggage, as well as new customer services are all part of the mix.

Bombardier's CSeries jetliner that carries Pratt & Whitney's Geared Turbo Fan (GTF) engine – an engine that comes with 5000 sensors that generate up to 10 GB of data per second. A single twin engine aircraft with an average of 12 hours flight-time can produce 844 TB of data. By the end of 2014, it was estimated that Facebook accumulates around 600 TB of data per day; but with an order book of over 3500 GTF engines, Pratt could potentially download zeta bytes of data, once all their engines are in the field. Therefore, It could come to pass that data generated by the aerospace industry alone could surpass the magnitude of the consumer internet.

The GTF engine uses great swathes of data to build artificial intelligence and predict the demands of the engine in order to adjust thrust levels. As a result, GTF engines are demonstrating a reduction in fuel consumption by 10% to 15%, alongside impressive performance improvements in engine noise and emissions.

The new generation of GEnx engines started pumping 5 to 10 TB of data per day. GE expects to gain up to 40 per cent improvement in factory efficiencies by the application of IoT and Big Data Analytics. Rolls Royce collects similar amounts of data from 12,000 engines across the globe into its data centre.

Bombardier recently announced that it has signed an agreement with Pratt to use their eFAST Health Monitoring System on the CSeries aircraft. Bombardier can earn more revenue by receiving data on the real-time performance of their engines, so they can adjust the way planes are flown and deal with potential issues before they end up grounding airplanes for larger repairs.

While engines are leading the charge and embracing IoT and data generation, avionics systems are also catching up to this trend quickly. The traditional avionics systems transfer data up to a maximum of 12.5 KB/s whereas Boeing 787 Dreamliners and A350s are using Ethernet-based, next-generation aircraft data networks, called AFDX that allows up to 12.5 MB/s.This makes it quicker and easier to transmit the information from avionics systems to the maintenance teams on the ground about current flying conditions, as well as any faults that have occurred during the flight.

The prospect of collecting, managing, analyzing and automating responses to this data place demands on both manufacturer and airline IT infrastructures. Rapid innovation development platforms and cloud solutions are required to manage this torrent of data and in identifying and servicing new aviation service revenue opportunities.

“The volumetric will grow exponentially as sensors, beacons, wearables all start beaming information, connecting to each other as well as enterprise applications. In addition, IoT environments work in real time. This mesh of big and fast data and real-time cadence will need to be addressed in the architectural framework,” says Emirates’ Chopra.

Challenges

Another issue will be the airline sector’s dependence on legacy systems. “Right now, there are a lot of competing technologies and frameworks out there when it comes to the

IoT. If you combine this with the legacy technology that many airlines face, there's a lot of work to be done on interoperability. The starting point is to build IoT gateways and application programme interface layers to ensure that you have a platform that you can build from," advises Virgin's Graham.

Greater demand for data means more connected aircraft systems, which in turn grows the cybersecurity challenge. "The high need for Internet connectivity for commercial avionics systems allows for a greater window of opportunity for malicious activities. This scare has especially been restrictive for developed economies after aviation industry-based terrorist attacks that have occurred in the past two decades," a TMR analyst says.

Another challenge will be security. "Securing connected machines has a unique set of complexities that are very different from protecting a data centre," says GE's Bartlett. "In addition to software platform security, there is a need for protecting critical infrastructure and helping to ensure the reliability of industrial internet operations for airlines and passengers."

References and Resources also include:

http://blogs.ramco.com/iot-aviation

http://indiatoday.intoday.in/story/sukhoi-30-aircraft-iaf-assam-tezpur/1/965118.html

https://www.ge.com/digital/press-releases/how-airlines-are-tapping-internet-things

https://www.thingworx.com/ecosystem/markets/smart-connected-products/aerospace/

https://channels.theinnovationenterprise.com/articles/7319-analytics-and-the-internet-of-things-in-aerospace

http://tass.com/science/960906