**Dr Sherif Sayed Ahmed** explains how a combination of advances in millimetre-wave communication and machine-learning algorithms has enabled the development of a high-performance security scanner that can detect concealed threats quickly and accurately

# SECURITY SCANN


Air travellers expect airport security to be visible and effective in preventing attacks. Feeling safe is an important part of the customer experience, but so too are speed, efficiency and privacy. It is tough for airport authorities to meet these apparently conflicting objectives simultaneously. Setting up extra lanes for security checks demands more space, equipment and staff. On the other hand, investing in more highly advanced technology must be done carefully: so-called "backscatter" X-ray machines introduced to perform full body scans at US airports in about 2011 had to be withdrawn from service after criticism from privacy groups.

Before the backscatter equipment was eventually removed, the US Transportation Security Administration (TSA) tried to overcome privacy fears by allowing travellers the option of a pat down as an alternative to the scan. This, of course, is slow, labour intensive and has obvious weaknesses that can be exploited. These disadvantages defeat the objectives of automated scanning, and work against delivering a good customer experience. A better solution is needed.

Millimetre-wave systems, which use radio waves, are known to be inherently safer than X-ray equipment. Even so, the images captured can be highly detailed leading to similar privacy concerns. The privacy problem arises for the same reason that millimetre waves are so effective at detecting threats: the waves can penetrate clothes, but are then broadly dispersed by the body's water-based cells. This results in a detailed image of the surface that can accurately highlight hidden threats including non-metallic objects such as plastic explosives or ceramic blades that are difficult to detect using other types of radiation. The downside is that more intimate

# NING MADE EASY


details can also be revealed.

Automating the analysis of images, to detect any concealed threats without inspecting actual body images, can not only help to protect travellers' privacy, but can also enhance threat detection by removing human error, as well as reducing instances of 'false positives'. Minimising false positives helps ensure checks are faster and queues are shorter.

Automated analysis, however, calls for high-speed real-time imaging and processing that has historically been beyond the scope of affordable commercial equipment platforms. The latest silicon-chip integration, combined with innovative management of millimetre-wave reflections and machine-learning algorithms, has now made it possible to realise a commercial, real-time, security scanner for automated high-speed 100 percent screening of airport passengers. The equipment can also be used for security screening in other transport hubs as well as border controls, security-conscious buildings, sports and entertainment venues, and anywhere rapid personnel screening may be needed to guard against concealed threats.

London City Airport recently announced it had installed one of these new systems, a R&S QPS200 Quick Personnel Security Scanner, which protects passengers' privacy by analysing data automatically in real-time and immediately discarding information that reveals no threat. No data is stored, and no actual body images are ever displayed on-screen. If a possible threat is detected, its location is displayed on a symbolic graphic of the human body, or avatar. The abstracted, impersonal image provides effective guidance for appropriately trained security staff to investigate further.

The R&S QPS200 brings together several innovations to achieve the extremely high speed and performance needed, in a cost-effective and reliable solution suitable for intensive daily use at the world's airports: London City Airport, which is relatively small, is using the system to help screen over 10,000 passengers per day.

The system uses an array of millimetre-wave transmitters that emit very low-power signals towards the person being scanned. Receiving units then analyse the resulting complex patterns. The transmitters must be positioned at close range to the body due to the illumination limitations caused by the specular reflections out of the human skin at the millimetre-wave frequencies. To scan the entire body would normally require a dense and, therefore, expensive array of individual transmitters, or a moving scanning mechanism that would not be fast enough to complete the scan in a short enough time. R&S QPS uses a new approach that clusters and positions a smaller number of transmit and receive antennas, and uses digital beam-forming, to create an electronically optimised aperture that ensures good image quality at close range.

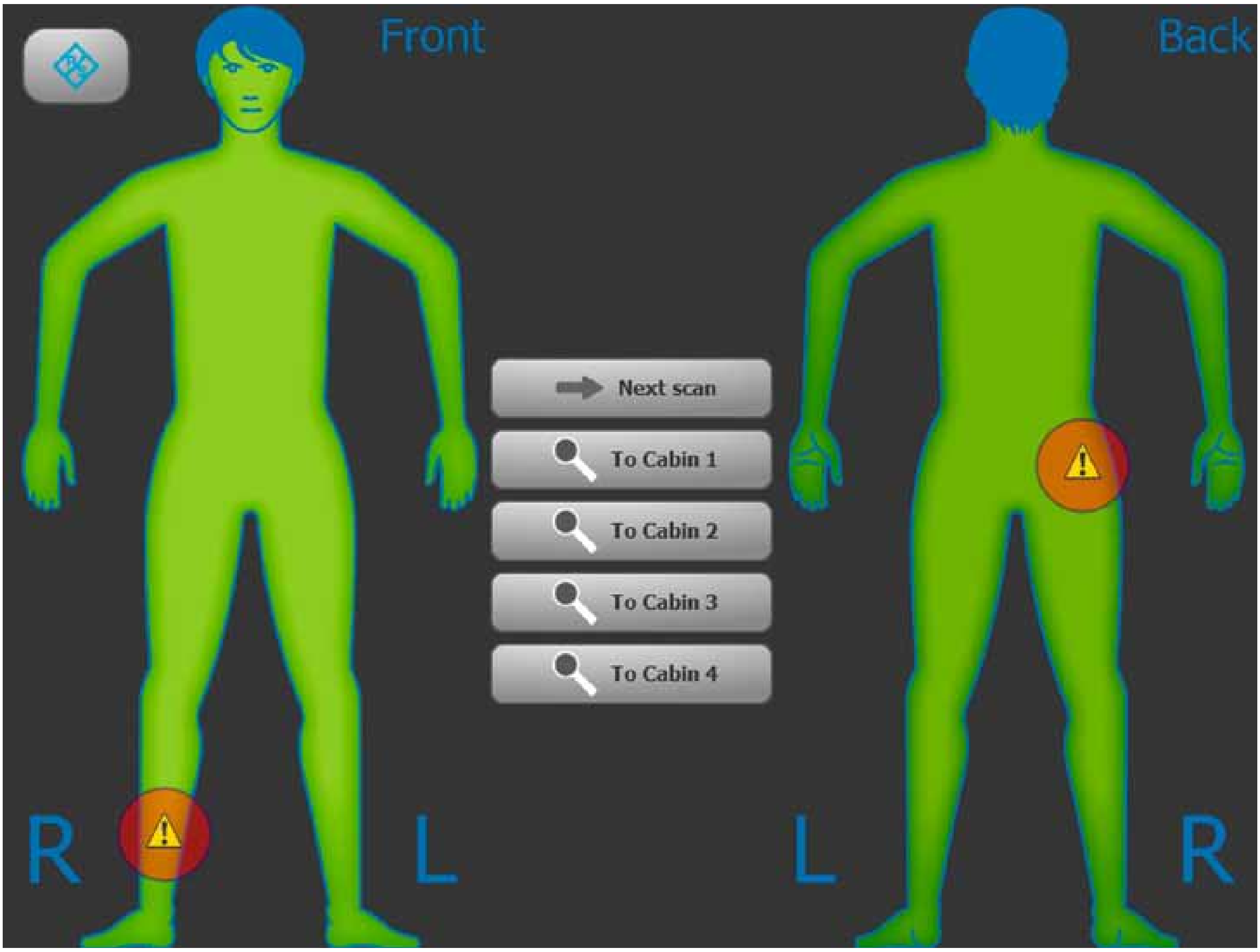
The finer points of the transmitter-receiver units (transceivers) hint at the close attention to detail that has made this high-performing scanner possible. Specially designed advanced signal sources, using digital techniques for accurate phase stability, ensure coherent sampling of the transmitted signals by the receivers. The antenna design is also optimised to ensure small footprint and high bandwidth.

In addition, the system operates at higher frequencies than conventional millimetre-wave systems, which usually operate at frequencies in the 30GHz range. Operating in the 70-80GHz frequency range (millimetre-wave frequencies are from 30GHz to 300GHz) allows a higher signal bandwidth resulting in superior range resolution. Choosing this frequency range also allowed the project to leverage existing IP developed for automotive 77GHz long-range radar systems.

Even using the inventive approach to minimise the number of transmitter/receivers needed, the security scanner requires multiple imaging clusters comprising a total of over 12,000 channels. Highly integrated electronics were required to realise the transceivers that are both cost-effective and reliable. For this part of the project, R&S teamed with semiconductor manufacturer Infineon to produce a custom RF front-end chipset comprising a four-channel transmitter and receiver. Other essential components like resistors and capacitors are also integrated in the device to minimise overall component count, solution size, and number of interconnects. The devices operate from a single 3.3V supply, and consume approximately 150mW per channel for the transmitter, and 180mW for the receiver when fully activated. Perhaps more importantly, from a safety point of view, the radiated RF power is about 1 milliwatt; equivalent to one-thousandth the signal strength of a mobile phone.

Developing these chips has been critical to achieving the performance needed to complete the front and rear scans simultaneously within milliseconds, to achieve the throughput rates necessary for a practical air-passenger scanning system. The ICs are implemented as Monolithic Microwave ICs (MMICs) using a silicon-germanium (SiGe) bipolar process. In the longer term a lower-cost solution based on similar CMOS technology to high-performance PC processors and DRAMs may be considered. This will depend on continued advancement of CMOS processes to deliver the required performance at the R&S QPS frequency of 75GHz and 10GHz bandwidth.

Four of the transceiver clusters are connected to a




signal distribution board, and combined with a power supply, mechanics, and cooling parts to create one unit. Eight units are combined to form a panel measuring two metres tall by one metre across, which can scan the front or rear of the passenger. A fully operational system has two panels, positioned in front and behind, to perform simultaneous front and rear scanning. These two panels are connected to a central industrial PC via fast PCI-Express connections.

The transmitters in each array illuminate the volume in front of the panel sequentially, and the complex reflected signals are simultaneously and coherently sampled by all receiver channels. These received signals are then digitally converted to a lower frequency for analysis, and digitally filtered in parallel to help minimise measurement time. The sampled data is processed, reflections are calculated, and system error correction is applied.

Because threat visibility is crucial for system performance, even the floor of the system, beneath the passenger's feet, is engineered to help maximise the signal strength at the receiver antenna. The floor is made of a dielectric layer bonded on a metal surface. The design of the structure is made specifically to rotate the signal polarisation to ensure it is co-polarised to the receiver antenna. This solution is based on patented technology and is not trivial to do. The surface is fully passive and robust for daily operation. Hence the floor is used as a mirror surface to extend the illumination coverage of the system and to enhance detection around the ankles.

The data for the digital image is reconstructed on a per-cluster basis, in parallel, to help reduce the extremely high internal data-transfer rates that would otherwise be necessary. Even using this technique, the data-processing load can be as high as 10.6 trillion operations per second to allow full image reconstruction in less than two seconds. The system can image features as small as a few millimetres in size, and can show depth variations down to 50 microns.

The image data is analysed automatically in near real-time using highly optimised and dedicated machine-learning algorithms that are tailored for such security-scanning tasks. Each part of the 3D image is analysed and observed to decide if any location looks anomalous to usual conditions. The algorithms are also trained in a manner that makes them more accurate in finding relevant threats, including but not limited to weapons such as explosives, guns or knives.

The latest advances in millimetre-wave imaging, combined with intelligent image processing, have enabled a convenient, cost-effective security scanning system that can be accepted by the travelling public while helping accelerate security checks, reduce errors, and enhance detection of genuine threats. We may see such systems become widely used, not only in airports but also in other transport hubs as well as offices, public buildings and entertainment venues.

***By indicating the position of any suspect objects on an avatar, the system displays potential threats without showing or storing any images of the scanned body***

**Doctor S Sherif Ahmed** is with Rohde & Schwarz in Munich, Germany where he specialises in modern microwave imaging technologies His current R&D activities include: near-field microwave imaging, stand-off imaging, along with the non-destructive testing, multistatic radar, advanced signal-processing techniques and terahertz technology.