Elusive and ambiguous, yet absolutely imperative to the survival of the industry, safety is a critical element in the world of transportation. We sit down with the resident expert at the faculty, Prof. John Stoop, to gain more insight into the world of accident investigation, forensic engineering and what safety actually means.

To start with, can you tell us a little bit about yourself and how you ended up at the Faculty of Aerospace Engineering?

I started studying Aerospace Engineering in this faculty in 1968 and did my PhD on the role of safety in the design process. For about fifteen years I worked at the Faculty of Technology, Policy and Management, I was the Dutch liaison for the Research and Development Corporation (RAND) team who did the investigation into the safety of Schiphol Amsterdam airport after the EALI crash in 1992 and also developed a multi-modal methodology for accident investigation. This gave me the opportunity to return to aviation and the faculty. During my application, the dean at that time, Ben Droste, asked me: “What is your capability which we need and don’t have in-house yet?”, and I said “Making safety explicit again as a strategic value and feed it back into the master’s course in Aerospace Engineering.” Then he said: “That is true, you’re hired.”

The two subjects you teach, Forensic Engineering & Safety of Transportation both deal with what happens when things go wrong – what drew you to this particular subject?

It wasn’t so much the safety issue, but the investigation issue. I found investigating safety, misfortune, failure, accidents fascinating because at the time I did my courses, we had several lectures by Professors Spies, Van den Berg, Taub and others who showed us how aircraft had failed, why they failed, and how failure could be traced back to the design process. Using a piece of wreckage, it was possible to demonstrate the failure mode, explain why a certain theory had been developed, how the aircraft had actually failed and what the solution could be. Such detective skills were already fascinating to me when I did my courses in aerospace engineering (AE).

Given that safety is paramount in the aerospace industry, do you think that it is a subject that should be dealt with in more detail during the course of the study (the courses are currently only available as electives in the Master programme)?

Very short and simple answer: yes. But why, of course, is the more important question. I became interested in this investigation methodology because investigation formed a part of my courses. It has been disappearing quite to an extent from this faculty, as it moved towards other forms of risk assessment and how to deal with safety in design and operations. But it is an indispensable part in high-tech development; as technology changes and evolves, this also needs to be reflected in safety, and how it is assessed and implemented.

‘Safety’ as a concept seems rather vague - how can you implement safety when designing an aircraft or spacecraft?

By combining the two approaches; forensic skills are the counterpart of design skills. Investigators start with the black
hole in the ground, designers start with a blank sheet of paper, but both focus on an optimal safety performance. As in any other field, it is important to establish a scientific basis for what you do. We use accident investigation as one of our analytic tools. After an accident, you visit the site, make observations, collect evidence, and then try to reconstruct what happened. You need to try and identify failure mechanisms, then come to certain conclusions. You link these conclusions back to the design phase and consequent-
ly to the operational phase. Closing this feedback loop from reality to design and operations is very important. You need to identify design decisions and their underlying assumptions and the transfer of residual risks and side effects to operators. Safety issues that cannot be dealt with during design should be covered during operations by procedures, training and mitigation of their potential consequences. When you find out that there are deficiencies in operation, you need to learn from them and see if a redesign of the aircraft and its operating procedures is feasible.

To integrate safety into a product or a sys-
tem, it is best to start from the beginning, but often that’s not possible. How effective/efficient is it when you have to do this retroactively?

That can be very effective as well, but you should know why the accident happened. That’s the forensics part of it; if you understand why people use their products in the way they do, then you have several options for improvement. You can change the products, but sometimes you can also change regulations and procedures to change the behaviour and train people to improve their skills. It is not restricted to strict engineering design; sometimes you have to provide a safety management system or change the organisation. Eventually, it is all customer-driven and cost-driven; we are able to redesign the entire system, but in practice, there are often restrictions on how much you can change.

I think it’s a case of going back to your roots. In particular in aerospace, safety was an accident investigation skill. As the industry grew, a variety of methods and schools of thought emerged, fragmenting safety as a strategic issue. But the core question has always been: "Why did the system fail?" So in order to regain oversight, you have to delve into safety critical details, you need to know what actually happened in specific cases under specific conditions. Then the old skills of investigating become popular again. But instead of old male detectives smoking pipes, the image now is of beautiful women with sophisticated labs and equipment. Investigating is becoming more of a scientific rather than a police activity, and that appeals to engineers and researchers. We can take advantage of the popularity of this new image of forensics.

Do you think that when it comes to transportation, and the companies involved, there is an inherent conflict between system safety and profit?

It depends on the level. If you consider the aviation industry where you need to maintain public confidence, safety is a
strategic value. But when you are an (air-line) operator or a pilot, you have to deal with the actual situation and balance all operational aspects. It means you have to fly out of Schiphol airport without using too much fuel, making noise, or disrupting passenger comfort. My concern is that because safety is hard to measure, it simply disappears from people’s minds. You may end up with sweeping statements like “Thou shall be safe” and leave it at that. There are too few tools to maintain oversight over safety, while there are many tools to maintain oversight over economics, pollution or noise. It is a challenge to express safety in terms of performance indicators and make these indicators tangible.

How do you think you could do that – make safety more tangible?

Bring back operator experience. The people who really get nervous when things may go wrong are the operators: pilots, air traffic control, maintenance and so on. They have a good professional judgement of what might go wrong. We have to feed back that expert judgement, operational knowledge and professional experience into the system in order to influence and balance the decision making and the design.

In a field like aerospace engineering which often involves cutting-edge technology, it is not always possible to know in advance how safety will be affected by any new technology. How should engineers address such an issue?

There’s a very simple answer: by documenting design decisions. It has been done in aviation to a large extent, but mostly with respect to components. We know the engines are reliable, the performance envelope is transparent, but remembering why you took a design decision and the knowledge which supported it, is most important. A lot of this knowledge only comes with experience, therefore input from pilots, maintenance crews, air traffic control and so on can also prove invaluable.

How much acceptable risk do you think one should take, for the promise of improved performance?

You cannot express that in a single number – it’s not that simple. Acceptability is also in dealing with how transparent you are in your decision making. If you document it well, if your uncertainties are clear – then you can identify weak areas and work on them. But that takes a lot of development because experience should be transformed into evidence-based knowledge. Therefore the knowledge based engineering (KBE) concept is so interesting. By incorporating designer and operator knowledge and experience in your body of knowledge, you can control uncertainties much better.

What about the issue of ethics in safety?

Ethics is an integral part of safety. Somebody said once, “We never leave our home in the morning and wonder how many passengers we should kill today.” The same should apply to designers and engineers. People get killed by the fact that we might be deficient in our design. It is not ethical for people to lie their lives due to the limitations of your assumptions.

You often hear at the faculty, “Aircraft have been the same for the last 40 years and they need to change drastically” – what kind of impact would such a drastic change in system have on safety?

That’s why it is so important that safety is recognized as a strategic issue for the faculty. It’s fascinating to see that we design blended wing bodies, hydrogen propulsion, composite designs, all kinds of high-risk things, but there should also be an advocate for safety involved in the design process, someone who will stand up and say, “Did you think about safety?” That is my role to some extent.

What do you think is the biggest challenge in designing a safe aircraft?

The biggest challenge lies in integration. You cannot engineer an aircraft on an expert-basis only, it’s a complicated system. In knowledge-based engineering, you need to know how to keep the balance between all design aspects.

If you were in charge of designing a new aircraft, having a well-integrated base of technology would be your main requirement?

Yes; if you’re missing a system integrator, you will run into serious problems. We have seen that with infrastructure developments in The Netherlands and perhaps even with the Airbus A380, it is so complex that you need people who have oversight and the ability to foresee. It was a
combination of design expertise and operational skills that diverted disaster after the A380 engine failure.

How do you think current trends in security will change the aircraft of the future? For example, do you think aircraft developers today will be focusing on making aircraft “terrorist-proof”?

Yes, definitely. There is a risk that we optimize around a single aspect that is popular at the time. Previously, for example, noise was a big problem, so now there are aircraft optimized for low noise emission. Then we had the terror threat. There are so many restrictions based on the optimization around just one aspect, that this may create an imbalance in the system.

So this imbalance is something that the aviation industry generally suffers from?

Definitely! Do you know how much money it costs to make Schiphol airport secure? Schiphol needs to be as open as possible to passengers 24/7, while at the same time as closed as possible to terrorists. That’s impossible! But we have to make it happen somehow, and in the end there will still be issues that are not taken into account.

But if some serious issue is overlooked and an accident happens, what then? Who is held liable?

If an engineer who designed an aircraft thirty years ago, will get the blame for an accident today, then there is a serious problem in the system. We can only do the best we can: to explicitly show what knowledge we have, what proof we provide and decisions we make, to document everything and try to be as open and as professional as possible.

So if you could design an aircraft in a sort of bubble, away from all the external influences and the pressure to satisfy everybody, do you think you could come up with an aircraft that was better than what we have now?

[laughs] Yes, I really think so. If you put experts in a room and wait for the ultimate design, you come up with something completely different than if you also invite laypeople and the public to that room. That is when engineering becomes a negotiation process, and you don’t want that. When the design of the product is complete, it should be handed over to stakeholders for assessment, but these parties shouldn’t be involved in designing the product. If safety becomes a negotiating issue in political decision-making, then we run into serious problems.

You always hear that in any system, the person behind the wheel is the greatest liability. There is the idea that unmanned cars would be safer because you don’t have that unknown factor. In your opinion, is that true?

No. You should create a better human-centred system, to mould their task to their abilities. I think that’s a better approach than leaving people out of the loop. We see this trend in aviation to some extent: pilots are flying an aircraft which is highly automated, but if something happens, they are assumed to take over, since they have the skills and training to deal with emergencies. People are better problem solvers than remote controllers.

Do you think that’s happening too much these days, especially in aviation, that flight systems are automated?

The two major recurring challenges for the community of safety investigators are software reliability and human performance. If you don’t rely on humans, you should have perfect software. But since there is no perfectly reliable software, you should have reliable people operating. You can never solve the problem by eliminating one of the two components of the system, because then the other will be lost as well. It is a matter of checks and balances.

What future do you see for safety investigation work at the faculty?

I would like to see three things at this faculty: Firstly, keeping the legacy of the professors who emphasized safety as a strategic issue. Secondly, we should try to learn from accidents and incidents as much as possible, through practising investigator skills by something like a crash laboratory or a forensic centre. In the past, students learned about accidents directly from wrecksages. We should bring that type of case-based learning back in the curriculum in a modern IT format. Finally, I would like to see forensic engineering and safety investigation integrated again in the master’s course we offer to our students, preferably in an international network of academia.