ABSTRACT: Due to its promising properties, hydrogen has become increasingly interesting for transportation applications. Nevertheless, possible applications also require answers to the question of how to establish and demonstrate sufficient safety to achieve society’s acceptance and approval of authorities. This paper addresses these questions and is organized as follows: First, we start with a short overview of basic properties of hydrogen and current ideas of using it for aircrafts and cars. After a review of basic risk and safety aspects we then discuss how risk strategies are realized within the automotive sector where the development has progressed significantly during the last years. Next, we describe the tolerable risk target for hydrogen in aircrafts. Finally, we discuss an overall approach which includes the basic philosophy of risk management, the already existing safety concepts, tools and methodologies and also the existing experiences of handling hydrogen in other industries.

1 BASIC PROPERTIES OF HYDROGEN AND ITS APPLICATION FOR THE TRANSPORTATION SECTOR

Hydrogen is considered an alternative fuel for three reasons: It is lightweight, renewable and it is the most abundant element on the earth. The major advantage of hydrogen is that it stores approximately 2.8 times the energy per unit mass as gasoline, i.e. it supplies more energy per unit volume than gasoline, diesel, or kerosene. There are several ways to extract the energy contained in hydrogen: By combustion (internal combustion engines, ICEs, or turbine engines) or by converting it to electricity in a fuel cell. Research and development projects have demonstrated that hydrogen is interesting to transportation applications today.

On the other hand, hydrogen shows a wide explosive range, coupled with very low ignition energy. The minimum ignition energy required to ignite a hydrogen mixture is just 0.02 mJ, which is equal to the energy of a static electric discharge from the arcing of a spark. Therefore, an accumulation of hydrogen in a poorly ventilated room can easily result in an explosion. These properties force us to consider also safety aspects when handling hydrogen. Nevertheless one also should not forget that the diffusion coefficient for hydrogen is about 0.61 cm$^3$/sec, which means that hydrogen mixes with air and disperses rapidly with no pooling on the ground – unlike petroleum-based fuels.

Performance evaluations show two favorable fuel cell (FC) processes for transportation applications, Proton Exchange Membrane Fuel Cell (PEMFC) and Solid Oxide Fuel Cell (SOFC). FCs use gaseous hydrogen (GH$_2$) which may be provided by
- GH2 in pressurized tanks,
- LH2 in insulated tanks,
- Reforming hydrocarbons.

Kerosene reforming is presently the preferred solution for aircrafts because only one fuel type (kerosene) is onboard, in addition with a 4 times higher density than LH2. To produce hydrogen from kerosene, steam reforming, partial oxidation and auto-thermal reforming are considered as possible solutions. Currently, the usage of hydrogen for auxiliary power units (APU) is of special interest for aircraft industry. On the other hand, reforming is no practicable solution for car, because hydrogen must be onboard in this case.

What about safety aspects?

1.1 The situation for aircrafts

In general, aircrafts must be engineered properly to minimize risks to the occupants, i.e. passengers and crewmembers. In commercial aircraft, safety is assured by first identifying hazards and then performing a fault hazard analysis. In this approach (see, e.g., Levenson 2003, FAA, EASA) the hazards are traced to the aircraft components with their re-
As well as experiences that manufacturers and suppliers are gathering with their internal solutions form the input for the standardization committees.

The standardization process has made progress in the last years (for a summary see Klein et al. 2004a), but is still not complete. Until specific technical rules are formally accepted, the design has to be developed according to the experiences with related engineering disciplines, e.g. with the transport of hazardous goods or with automobiles using liquefied gas (LPG) or natural gas (CNG) (see NGV-requirements). The final goal is, of course, to make life easier for suppliers and manufacturers: Following an accepted standard usually implies that associated risks are in fact tolerable. So we need two things: A risk target and experience that the target is met in practice. But exactly these prerequisites are missing and it is even not expected that an automotive standard will define a risk target.

So with respect to standardization the situation is more advanced compared to aircraft industry. But there are also big differences between the two “worlds” of aircraft and automotive industry. This is essentially due to the fact that cars are a mass product, whereas aircrafts are ordinarily not built in huge number of pieces. Some important implications (among others, of course) are:

- Aircraft crews are very well trained people and fully aware of safety-issues. Ordinary drivers usually do not read carefully operating manuals and just want to start their car and drive — otherwise, if they have to wait for some time — they may be tempted to repair off one’s own bat … That is, the user aspect is by far more relevant for cars than it is for aircrafts.

The specific engineering solutions to operate a LH2- or GH2-fuelled car are also different from aircrafts, because hydrogen must be stored within the car. If leaks or ruptures occur — they may be spontaneous or due to external events like in the case of a road accident —, they lead to uncontrolled release of hydrogen. Therefore, to avoid associated hazards, the system must be designed adequately: Components like the tank, valves, pumps, piping systems, casings, sealing must be properly designed with respect to material, temperature and pressure of the medium. Normal operating conditions as well as accident scenarios with corresponding dynamic and static loads must be taken into account. Safety functions like shut-off- or release-valves, sensors, control equipment must be scheduled to warn in the case of uncontrolled release or keep it as low as possible.

But what does “designing a car adequately” really mean? Certainly one has to observe “sufficient safety”, but also to avoid over-engineering.
2 BASIC ASPECTS OF RISK AND SAFETY

How shall we deal with the unavoidable residual risk? It cannot be ignored and must be accepted by the authorities and society. Of course, the question arises of how to define acceptable risk and how it can be validated that the system is “safe enough”.

Following the standard terminology risk can be defined as combination of the probability of occurrence of undesirable consequences and their severity (IEC). Such undesirable consequences can be physical injury or damage to the health of people, damage to the environment or to property.

It is useful to distinguish between “risk” and “hazard”: Hazards exist as source with a potential to cause undesired effects to human, property and the environment (potential risk). The risk, on the contrary, includes the likelihood under which this source causes damage. With the use of adequate protective measures, risk can be reduced. Risk, therefore, depends not only on the hazard, but also on the protective measures taken against the hazard. These measures do not only include technical solutions, but also human intervention and risk management. The answer to the question “What would be the adequate protective measures so that the level of (actual) risk from a given hazard (potential risk) will be low enough (lower than a given threshold)?” is certainly one of the most important issues of risk analysis.

Without any protective measures, each hazardous state would immediately result in negative consequences. The resulting risk of the equipment considered would be usually too high compared to a given tolerable risk target.

To achieve safety, the risk must be reduced by suitable functions (“safety functions”, IEC) which are intended to achieve or maintain a safe state for the system. Physically, these safety functions are realized by technical systems (e. g. electrical/ electronic/programmable electronic (E/E/PE) systems). There is a certain (hopefully high) probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time. Following IEC, this probability is called “safety integrity”.

Several well established methods can be used for calculating the probability of dangerous failures of the system: Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), Markov Analysis, System Simulation using Monte Carlo Methods. The methods are well known and shall not be discussed here again together with their advantages and drawbacks. In our context, it is important to note that the different methods have one thing in common: They describe quantitatively the probability (or rate) of certain failure modes and the effects of failures of the main components by a logical analysis of the functional dependencies between the components. Failure modes together with the component form the “basic elements” of the analysis, and corresponding failure rates or failure probabilities for these elements have to be fixed then. We need quantitative values for the rates or probabilities, or, to be more precise: The parameters are not fixed values, but continuously distributed random variables and the relevant distributions are characterized then by form-parameters, mean values, standard deviation etc. Thus one needs a function with several parameters just to describe one failure mode for one component. To derive such a function requires a broad operational experience with the component at comparable ambient and operational conditions.

Besides technical solutions, an overall risk analysis also takes into account other “barriers”, e.g. rules, procedures and process knowledge of the operators or unplanned circumstances likely to avert or mitigate negative consequences.

Consequence analysis summarizes the barriers which have to become active to avoid that a hazard develops into a damage state. Human actions acting as barriers can be treated in quite a similar way as technical failures by using human error probabilities which can be derived from data collections or described by so called operator action trees. Eventually, in order to determine the extent and type of consequence (i.e. harm, injury, and damage) in the case of hydrogen release, CFD-calculations, fire or explosion models and vulnerability models are used.

The risk analysis ends with statements about the likelihood of certain critical events and their resulting consequences, i.e. (simplified) with “points in the risk diagram” of figure 1. Each region of the diagram requires specific action: In the “unacceptable band” risk must be reduced at whatever costs. In the “acceptable region” little or no effort is justified to reduce it further. Somewhere in between the procedures for measures can be characterized by the ALARP- (“as low as reasonably practicable”) principle. In the UK and the Netherlands, e.g., for process industry some form of Cost-Benefit-Analysis is recognized as a relevant approach to derive what is relevant and what is not.

What is the situation in the transportation sector?
3 AUTOMOTIVE INDUSTRY

As discussed in chap. 1.2, we have no general regulation, no general accepted risk target and no extensive operational experience with hydrogen cars. In the moment, hydrogen cars are more or less prototypes, operated by specially instructed people, but as we already emphasized a car must be suitable for ordinary users, not for hydrogen experts.

Even if we had defined a risk target and series production with thousands of hydrogen cars shall start in the next decade, the statistical basis for incidents or accidents will probably be still too small to verify that the risk target is achieved.

That’s why we applied another solution to define the tolerable risk target when we analyze hydrogen cars (Klein et al. 2004b): We compared the risk for the hazard of fire of a conventional car with the corresponding risk for fire or explosion for a hydrogen car. The argument is simply that the consequences – injured or even killed persons by fire or following an explosion in a car – are similar in effect and therefore should also be so in society’s perception (a similar approach, the GAMAB-Principle, has been formulated for railways, see CENELEC).

The general strategy is shown in figure 2 on the next page. Without optimization, the risk of new technical solutions usually will be higher than for the old solution, which, as we assume, was accepted by society. We must achieve that the new situation is (at least) “as good as before”. This means, we have to perform a comparative risk study.

Realizing an identical level of safety does not guarantee that the car is really accepted by society or its representatives, of course. But the criterion gives a hint whether it could be accepted and will be a well based argument for discussions, e.g. with authorities.

A common safety problem for hydrogen cars is, e. g., parking in a building or garage. Because the car could well stay there for some weeks, also small leaks can result in an explosive mixture of air and hydrogen.

Obviously, the parking problem does not exist for aircrafts which will probably produce their hydrogen on demand. On the other hand, an accident involving an aircraft attracts more attention than a car accident. If hydrogen is identified as cause of such an accident, the technology could be quickly refused by the public.

Correspondingly the safety requirements for automotive applications are in many ways very different compared to aircrafts. But there also some similarities, as we will see immediately.
4 TOLERABLE RISK TARGETS FOR HYDROGEN IN THE AIRCRAFT SECTOR

It is not necessary to adopt the approach of comparative risk analysis for cars to aircrafts, not only because of the differences we already discussed in chap. 1.2 but also because we have already well-defined tolerable risk targets in the aircraft industry which means a main difference to risk assessments for cars. FAA and EASA introduced the risk-concepts of “Probability of Failure Condition” and the “Severity of Failure Condition Effects”. The relationship between them is such that

(1) Failure Conditions with no safety effect have no probability requirement.
(2) Minor Failure Conditions may be probable.
(3) Major Failure Conditions must be no more frequent than remote.
(4) Hazardous Failure Conditions must be no more frequent than extremely remote.
(5) Catastrophic Failure Conditions must be extremely improbable.

These qualitative descriptions are completed by quantitative targets (FAA).

Catastrophic failure conditions, i.e. conditions, which would result in multiple fatalities, usually with the loss of the airplane, are of special importance. The regulations in AMC 25.1309 (System Design & Analysis, corresponding to AC 25.1309-1A), paragraph 8 (EASA), read as follows:

“c. The safety objectives associated with Catastrophic Failure Conditions, may be satisfied by demonstrating that:

(1) No single failure will result in a Catastrophic Failure Condition; and
(2) Each Catastrophic Failure Condition is extremely improbable.

d. Exceptionally, for paragraph 8c(2) above of this AMC, if it is not technologically or economically practicable to meet the numerical criteria for a Catastrophic Failure Condition, the safety objective may be met by accomplishing all of the following:

(1) Utilising well proven methods for the design and construction of the system; and
(2) Determining the Average Probability per Flight Hour of each Failure Condition using structured methods, such as Fault Tree Analysis, Markov Analysis, or Dependency Diagrams; and
(3) Demonstrating that the sum of the Average Probabilities per Flight Hour of all Catastrophic Failure Conditions caused by systems is of the order of $10^{-7}$ or less (See paragraph 6a for background).”

It is now interesting to see that the argument given at the aforementioned paragraph 6a is rather similar to the approach we discussed above with regard to automotive applications:

“Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 percent of the total were attributed to Failure Conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. (Highlighted by authors) It is reasonable to expect that the probability of a serious accident from all such Failure Conditions be not greater than one per ten million flight hours or $1 \times 10^{-7}$ per flight hour for a newly designed aeroplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. For this reason it was assumed, arbitrarily, that there are about one hundred potential Failure Conditions in an aeroplane, which could be Catastrophic. The target allowable Average Probability per Flight Hour of $1 \times 10^{-7}$ was thus appor-
tioned equally among these Failure Conditions, resulting in an allocation of not greater than $1 \times 10^{-9}$ to each. The upper limit for the Average Probability per Flight Hour for Catastrophic Failure Conditions would be $1 \times 10^{-9}$, which establishes an approximate probability value for the term ‘Extremely Improbable’=".

We can now argue that for demonstrating that the implementation of a “new system”, namely the “hydrogen system”, is not an intolerable risk, we have to stay below the threshold of the “tolerable risk target” of $10^{-9}$/flight-hour for the hydrogen system.

What is the hydrogen system in our case? For illustration, consider a fuel cell with hydrogen production by reforming. What must be analyzed in more detail are components like the reformer, the fuel cell or the piping system, but also the process control and monitoring system or safety instrumentation.

Existing concepts schedule a more or less complete enclosure of components or subsystems containing hydrogen. Furthermore, a completely autarkic system is planned, i.e.: All safety-related functions, e.g. controlled shut-off, must be performed fully automatically.

To demonstrate that we achieve our risk target we now have to perform a risk analysis (paragraph 8d(2) and (3) of AMC 25.1309) and use well proven methods for the design and construction of the system (paragraph 8d(1) of AMC 25.1309).

What could be done to realize this strategy?

5 IMPLEMENTATION OF RISK STRATEGY

The predominant hazard states which must be controlled and which are important for our case can be easily characterized and are similar to those in industrial fire protection (Barry):

- Loss of Containment
  
  Prevention, isolation, or shutdown of releases from explosive or flammable gas transfer systems (piping, pumps, process equipments like the reformer, fuel cell etc.)

- Process Safe Operating limits

  Prevention of process deviations (i.e. operating outside safe operating limits) that could lead to over-temperatures, overpressures and as a consequence loss of containment of process materials, e.g. hydrogen from the reformer in our case

Therefore, we first have to judge or estimate the probability of these hazard states. To do so, the special design of the hydrogen-system and relevant components (e.g. FC, valves, piping) must be defined. In the moment, generic data are essentially available just for stationary equipment; component specific data have not been published up to now, the statistical basis would probably be too small any-

way. This means an inevitable inaccuracy for the final results which must be evaluated.

In principle, we have two types of safety functions which prevent the hazard states from escalating into a real damage:

- Ventilation and inerting
  
  Prevention and control of flammability and combustible or explosive mixtures stemming from process upsets and loss of containment

- Emergency Control Systems (ECS)
  
  Used for pre-fire or pre-explosion mitigation and designed to control, isolate or shut down process equipment following detection of an abnormal event situation – the release of hydrogen due to failures of the enclosure in our case.

Again, the judgment on these systems, their application and functional performance requirements will depend on the actual design defined, specific scenario and the established risk tolerance criteria.

To meet these performance levels, reference to IEC 61508 (IEC) can be made for the ECS. This standard treats safety instrumented systems (SIS) in general terms. A SIS is generally composed of sensors, logic systems and actuators for the purpose of taking the system to a safe state when predetermined conditions are violated.

What performance can we expect? To illustrate this point let’s take as a (very) simplified example the release of hydrogen by a leak within the hydrogen system of an aircraft. The system is designed in such a way that a sensor detects gas and then activates the fire protection system. From a “classical point of view” the problem of hydrogen leakage is solved and the safety functions (sensor, protection system) are built, maintained and implemented according to the “state of art” (in reality, the design described here would not be sufficient from a “classical point of view”, of course).

For a quantitative risk analysis we first have to find appropriate data. Let’s take the following plant failure data which are derived from a LNG plant (CCPS):

<table>
<thead>
<tr>
<th>System</th>
<th>Operating or In service* hours</th>
<th>Major failures</th>
<th>λ [h⁻¹]</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard detection systems (sensors)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas detectors</td>
<td>16,703,000</td>
<td>44</td>
<td>2.6·10⁻⁶</td>
<td>Bayes</td>
</tr>
<tr>
<td>High temperature detectors</td>
<td>8,418,000</td>
<td>0</td>
<td>5.9·10⁻⁸</td>
<td>Bayes</td>
</tr>
<tr>
<td>Fire protection systems (final elements)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using gas</td>
<td>364,000*</td>
<td>2</td>
<td>5.5·10⁻⁶</td>
<td>Bayes</td>
</tr>
<tr>
<td>Using foam</td>
<td>88,000*</td>
<td>0</td>
<td>5.7·10⁻⁶</td>
<td>Bayes</td>
</tr>
</tbody>
</table>
For the Logic System we assume an arbitrary value of $1 \cdot 10^{-5}$/h and for all components a test period of one year. From table 2 we find that the SIL of the logic system is 3, for the sensor and the final element it is SIL 1.

Table 2. Safety Integrity Levels (SIL): target failure measures for a safety function, allocated to an E/E/PE safety related system operating in low demand mode of operation (from IEC 61508, part 1).

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Low demand mode of operation (Average probability of failure to perform its design function on demand)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-4} &lt; 10^{-3}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-3} &lt; 10^{-2}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-2} &lt; 10^{-1}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-1} &lt; 10^{0}$</td>
</tr>
</tbody>
</table>

If the system forms a simple series connection, we find for the total architecture again SIL 1. To judge whether this is “sufficient” let’s assume that the ECS (or SIS) must guarantee a risk reduction of about 100 or more, corresponding to SIL 2. In this case, we can conclude that a second and redundant gas sensor and redundant fire protection systems are indispensable. A detailed investigation with respect to qualification and reliability of the components could also show that halving the periodic testing interval for sensor, logic and final element are further possible solutions.

The essential point is that we can now decide on a sound basis what to do. And even more, we can take the input data (which might look strange – what has a LNG-plant to do with hydrogen in the air?) and use them as reliability requirements for our suppliers – at least with respect to failure rates (of course, other items like EMC, ambient and medium temperature and pressure, vibrations etc. are also very important input variables for this purpose). For a more detailed discussion of standardization and certification see Klein et al. 2004a.

What has been said above holds equally for car and aircraft safety (although fire protection systems are not installed in cars). Another aspect is important especially for aircraft industry: Boeing and Airbus define many of the technical specifications for their planes based on their own internal standards. One should be aware of the fact, however, that aircraft industry cannot develop “stand-alone-solutions” without referring to well established codes like IEC 61508 – at least when introducing complete new technology with safety relevance. It wouldn’t be even wise to do so just because these regulations should not be regarded as formal restrictions but also as transparent basis for developers on the part of the suppliers and manufacturers.

6 SUMMARY

Considering the present situation of introducing hydrogen in the aircraft and automotive industry, we draw the following conclusions:

- **Experiences** with hydrogen are available for cars, but these experiences and those of other sectors are only partly of use for aircrafts. Technical boundary conditions and the qualification of users are very specific for each application.
- **Standardization** is on the way, but there is no obvious cooperation of the big manufacturers in contrast to the automotive industry.
- There seem to be no fundamental difficulties with the introduction of hydrogen for aircrafts or cars with the regard to the technical equipment to be used.
- Nevertheless, more detailed analyses of the - process technology to be used, - E/E/PES and - fire protection measures are still necessary to guarantee the required level of safety. Insofar also learning from each other and from existing solutions is encouraged, with regard to engineering and standardization.

REFERENCES


CENELEC, Railway applications – Systematic allocation of safety integrity requirements, CENELEC Report R009-004

CCPS (Center for Chemical Process Safety), Guidelines for Process Equipment Reliability Data, with Data Tables, AIChE, New York, NY 1989

EASA, CS-25, Large Aeroplanes, Decision 2003/02/RM of the Executive Director of the Agency of 17 October 2003 on certification specifications, including airworthiness codes and acceptable means of compliance, for large aeroplanes

FAA, FAR Part 25; AC-25.1309

IEC 61508, Functional safety of electrical/ electronic/ programmable electronic safety-related systems, parts 1 to 7


Klein, G., Weidl, T. & Ortenburger, J., Hydrogen Applications in the Automotive Sector – Application of Risk Analysis, Chemical Engineering Transactions, Vol. 4, 2004

Levenson, N., 2003, White paper on Approaches to Safety Engineering