HyApproval

WP4 - Safety

Deliverable 4.7: Safety documentation for Handbook
&
Deliverable 4.10: Agreement on safety documentation

- PUBLIC -

Guidance for Safety Aspects of Hydrogen Infrastructure Projects

Version: 1.0
November 2006

HyApproval gratefully acknowledges the contribution from NREL (Jim Ohi) in providing the document from the U.S. Department of Energy: Hydrogen, Fuel Cells & Infrastructure Technologies Program entitled 'Guidance for Safety Aspects of Proposed Hydrogen Projects' (October 2005), on which these HyApproval Deliverables are based.

HyApproval D4.7 & D4.10 were prepared by Shell Hydrogen B.V.; additional comments were received from WP4 partners: ENI & Hydro

Table of Contents

Guidance for Safety Aspects of Hydrogen Infrastructure Projects

1. Overview

HyApproval gratefully acknowledges the contribution from NREL (Jim Ohi) in providing the document from the U.S. Department of Energy: Hydrogen, Fuel Cells & Infrastructure Technologies Program entitled 'Guidance for Safety Aspects of Proposed Hydrogen Projects' (October 2005), on which the HyApproval Deliverables D4.7 and D4.10 are based.
The US DoE document has been used to prepare these HyApproval deliverables as the information is seen as a very good example of best practice exchange between the HyApproval partners in promoting international harmonization for the development of hydrogen infrastructure projects. Only the specific references to US DoE hydrogen project solicitations, local US codes and standards and US terminology have been changed from the original DoE document.

This guidance document provides applicants with clarification on safety requirements for hydrogen refuelling station (HRS) infrastructure projects.
The document explains the objectives that must be met and provides examples, but it does not outline the detailed steps that must be completed in a safety plan. The responsibility of selecting and using a specific safety methodology falls upon the applicant or HRS infrastructure provider. A variety of practices exist for the identification and analysis of safety hazards, and the HRS infrastructure providers can choose an approach that is best for their project.

Safe practices in the production, storage, distribution, and use of hydrogen are essential for regulatory approval and for the widespread acceptance of hydrogen technologies. A catastrophic failure in any hydrogen project could damage the public's perception of hydrogen and fuel cells and could also decrease the ability of hydrogen technologies to gain the approval of the local regulatory authority, a necessary occurrence for commercialization. The HyApproval Handbook provides for practices and awareness that will result in an environment where safety is an integral component of HRS's.

A safety plan identifies immediate (primary) failure modes as well as any secondary failure modes that may come about as a result of other failures. In such a plan, every conceivable failure is identified, from catastrophic failures to benign collateral failures. Identification and discussion of perceived benign failures may lead to the identification of more serious failures.

All potential hazards in a hydrogen production, delivery, utilization, or storage system must be identified and analyzed, as well as any system aspects that may be adversely affected by a failure. These aspects include threats or impacts to:

- **Personnel.** Any hazards that pose a probability of injury or loss of life to personnel and the public at-large must be identified and eliminated or mitigated. A complete safety assessment considers not only those personnel who are directly involved in a HRS, but also those who may not be involved in the HRS at all, but are still at risk due

to these hazards, e.g. the safety assessment should also cover emergency services that may have to respond to a HRS incident a so as not to expose them to undue risk.

- **Equipment.** Damage to or loss of equipment or facilities must be prevented. Damage to equipment can be both the cause of incidents and the result of incidents. An equipment failure can result in collateral damage to nearby equipment and property, which can trigger additional equipment failures or even present additional risks. A complete safety plan must consider and minimize serious risk of equipment and property damage.
- **Business Interruption.** The prevention of business interruption, in addition to property damage, is important for commercial entities. Hazardous events may lead to interruption in providing service or product. This interruption is frequently expressed in terms of elapsed time before resumption of service or manufacturing. This time element can also be converted into euros as a loss of revenue, or value added. A complete safety plan in those instances would include time element interruption, and where critical, include a contingency plan for providing needed services or manufacturing.
- **Environment.** Damage to the environment must be prevented. Any aspect of a natural or built environment that can be harmed due to a failure should be identified and analyzed. A qualification of the failure modes resulting in environmental damage must be included in the safety plan.

2. Required Safety Plans

All plans for hydrogen infrastructure projects should include a preliminary safety plan or summary. All HRS infrastructure safety plans should include a sign-off page with the signature, name, title and division/department for those individuals (including the project manager) required to approve a safety plan as a project deliverable.
Safety plans should cover the work of any subcontractors and other suppliers and participants.

3. Preliminary Safety Plans

The preliminary safety plan needs to include the use of methodologies for identifying and analyzing safety risks, for mitigating these risks, and for communicating safety events to the necessary parties. The following items must be included in the preliminary safety plan.

3.1 Identification of Safety Vulnerabilities (ISV)/Safety risk assessment

A. The formal means by which potential safety issues on major process steps, operations and facilities will be identified should be outlined. There are several options for how this identification and analysis may be accomplished. The following options are suggested, but similar methods and analytical techniques may be used as well.

1. Rapid Risk Ranking
2. Preliminary Failure Modes and Effects Analysis (FMEA)
3. “What-if” analysis
4. Comprehensive identification and classification hazard analysis
5. Hazard and operability analysis (HAZOP)

6. Checklist analysis
7. Fault tree analysis
8. Event tree analysis
9. Probabilistic Risk Assessment (PRA)
10. Layer of Protection Analysis (LOPA)
11. Quantitative Risk Analysis (QRA)
12. Appropriate equivalent methodology

These ISV methodologies and analysis tools are further discussed in Section 4.1 Identification of Safety Vulnerabilities (see Page 5).

B. In addition to the preliminary ISV evaluation, a plan for preparing the final analysis or assessment that identifies significant safety concerns should be included. Published data on potential failures, rates of failure and failure frequencies and means of prevention and mitigation should be used when available. If data are not available, best engineering practices may be used.

3.2 Outline of the Risk Mitigation Plan that will apply to the project based on the preliminary ISV/Safety risk assessment. The Risk Mitigation plan should include the following:

A. **Description of how safety performance will be measured and monitored** to ensure that the ISV/ Safety risk assessment is updated regularly as data become available. The description should discuss how changes and modifications affecting safety will be screened and implemented including written procedures to manage changes to chemicals and other materials, technology, equipment, and operation procedures; and any changes to the facilities that affect the operation. The Management of Change (MOC) procedures should ensure that the following considerations are addressed prior to any change:

- The technical basis for the proposed change,
- Impact of change on safety and health,
- Modifications to operating procedures,
- Necessary time period for the change and
- Authorization requirements for the proposed change.

B. **Description of method to establish and maintain safety documentation.** This information should pertain to the process technology as well as equipment, chemicals and other materials being used in the process. It should include how maintenance records will be collected and/or automated and what data on reliability (e.g., damage mechanism, mean time between failures, failure effect, etc.) will be obtained.

C. **Description of Standard Operating Procedures.** The proposal should outline the steps that have been and will be taken to develop and maintain Standard Operating Procedures (SOP). SOPs should be developed, documented, and

implemented for each process with the active involvement of HRS infrastructure personnel. These SOPs should provide clear instructions for conducting processes in a safe manner. They should include:

- Steps for each operating phase,
- Operating limits,
- Safety considerations,
- Safety systems and their functions and
- Emergency shut-down.

SOPs should be readily accessible to personnel involved with the process, and be updated regularly to reflect any changes to chemicals and other materials, equipment, technologies, and facilities.

D. **Description of Employee Training.** The proposal should include a description of how safety training (with emphasis on hydrogen-specific training) will be administered to all employees working on the HRS installation, including all activities, such as, but not limited to personnel involved in inspection, testing, maintenance and emergency personnel. Training encompasses initial training, training on changes, and refresher training. A means for two-way communication should be established to enable personnel to communicate their safety concerns. A discussion of how training will be documented should be included.

E. **Description of Procedures to Ensure Equipment Integrity.** The proposal should outline the procedures by which the integrity of HRS infrastructure equipment will be assured at initial commissioning and through on-going maintenance, inspection and testing. The plan should identify how and when any identified deficiencies are to be corrected.

F. **Emergency Response Plan.** The proposal should outline provisions for the emergency response plan for the facility, neighboring occupancies and/or the public at-large, as applicable.

3.3 Outline for the Communications Plan that the HRS infrastructure provider will develop and implement during the project. This plan should include a description of:

A. Safety reviews to be conducted during the design, development and operations phases of the HRS development, the involvement and responsibilities of individual HRS infrastructure staff in such reviews, and how the review documentation will be reported to the local regulatory authority and to other pertinent organizations, and
B. The reporting, investigative and learnings process for each incident which resulted in, or could reasonably have resulted in, an unintended release of hydrogen or injury to people, equipment or the environment (see definitions and discussion on Page 13).

4. Safety Plan Preparation

Project safety plans need to describe the use of methodologies for identifying and analyzing safety risks dealing with main process steps, operations and facilities, the approaches for risk control, and the process for reporting safety related incidents and accidents to the necessary parties.

Safety assessments performed as part of developing a safety plan can take a number of approaches. One approach is noted here:

1. Perform safety assessment before construction begins—during design phase. Maintain construction oversight throughout the project.

2. Review system design against pertinent existing relevant regulations and standards (ISO, IEC, NFPA, etc.) and/or best engineering practices (e.g. EIGA guidelines, http://www.eiga.org/).

3. List hazards and safety issues. Which of these additional hazards and safety issues are of greatest concern to this particular project? Explain the basis for prioritization.

4. Develop accident scenarios based on risk assessment studies describing process malfunctions, human errors, system failures, etc. that could result in unwanted or unacceptable consequences from the hazards and issues identified in Steps 2 and 3. These scenarios can be prepared without regard to existing design safety features. For each scenario, the impact to personnel, equipment, business interruption or environment should be assessed both with and without credit for existing active mitigation systems (systems that require mechanical, human, or electrical actuation or intervention.)

5. Identify and correct construction and approval problems and deviations

    a. Identify and brief appropriate regulatory or statutory authorities early in the project (site/location specific).
    b. Address mechanical and/or electrical issues, storage separation distances, component ratings, ventilation, etc, as fit for purpose.
    c. Identify “new” hazards, if any—some hazards are equivalent to other commonly accepted public and industrial hazards
    d. Hazards can be characterized in terms of form, quantity, and location.

General guidance, requirements and examples for preparing the safety plan are covered below.

4.1 Identification of Safety Vulnerabilities/Risk assessment studies

As previously stated, the Risk assessment studies/Identification of Safety Vulnerabilities (ISV) can be in the form of any one or more of several different methodologies as chosen by the HRS infrastructure provider. This demonstrates that they have assessed and

integrated safety into the proposed project at the earliest stages. The methodologies are all established industry practices for safety and/or reliability engineering. The purpose is to analyze design components and system-level interactions for safety hazards and to demonstrate an understanding and anticipation of component failures. The most important objective is the prevention of problems before they occur. In the case of a failure, the Risk assessment study/ISV will lead to minimizing the effects of that failure. In a sense, it is a reliability tool as well as a safety tool, as it can help to identify areas within a system that are prone to failure.

Prior to performing the Risk Assessment study/ISV, efforts should be made to compile information central to the system. Pertinent information includes:

- Process flow diagrams
- Process and Instrumentation diagrams (P&IDs)
- Trip and shutdown systems
- Operation and emergency procedures
- Area safety drawings
- Chemical data sheet
- equipment types and location (indoors, outdoors, laboratory hood, etc.).

Information available from earlier HRS infrastructure projects may be effective in the collection of the above information.

The following sections provide descriptions and examples for various Risk Assessment/ ISV methodologies.

FMEA

Various methodologies exist for the performance of a FMEA, and numerous FMEA guides are available from traditional industry sources. In addition, websites such as **http://www.fmeainfocentre.com/** (a non-commercial web-based inventory dedicated to the promotion of Failure Mode and Effect Analysis) may provide additional information on the development of FMEAs.

In general, the FMEA process follows a standard procedure, as detailed below:

1. Identify top level hazards/events
2. Identify related equipment/components/processes
3. Identify potential failure modes and effects
4. Identify design inherent safety
5. Identify potential prevention and/or mitigation corrective actions

This outline is repeated for every component of every system. System-level failures must be included as well, as there are cases where every component may work well individually, but the system still fails.

A FMEA can be performed via two different approaches. The hardware, or component,

analysis is the identification and analysis of ramifications of component failures. This method is a bottoms-up approach, wherein failures are initiated on the subsystem level. The functional approach is a top-down method, starting at the system level. This is more suitable when specific components have not yet been chosen. Either approach is acceptable; both may be best in some cases. The development of the FMEA is a continuous process, and the document should evolve as the system design changes. A discussion and worked example of a FMEA can be found in *Guidelines for Hazard Evaluation Procedures*, a publication of the American Institute of Chemical Engineers (Ref 1).

"What If" Analysis

The methodology behind a "What If" analysis is a speculative process where questions of the form "What if … (hardware, software, instrumentation, or operators) (fail, breach, break, lose functionality, reverse, etc.)..?" are formulated and reviewed. The method has as its basic features:

1. the scope definition,
2. the team selection,
3. the review of documentation,
4. facilitated question and response evaluation with consequences, (which includes the likelihood rating, the release-severity rating, and the risk-based assessment classification) and
5. summary tabulation to the set of questions.

The "What If" questions are facilitated during a team review of segmented sections of equipment found in an engineering drawing (such as the piping and instrumentation diagram, P&ID) and/or for each step in an operating procedure. The team review usually focuses on each individual segment as the basis to ask and respond to questions as a group. Questions are formulated in the style of the question, "What if .... ?" The questions should address the following types of actions:

- Equipment failure,
- process condition upsets due to temperature, pressure, or feed upsets,
- instrumentation failure,
- interfacing utility failures,
- operator timing, out-of-order sequencing, endpoint failures, or inattentive departures from operating procedures during normal operations,
- start-up or shutdown maintenance related accidents
- site related events, such as handling related accidents,
- third party events such as accidents or storms.

A good example of a "What If" analysis can be found in Ref 1.

HAZOP

The Hazard and Operability Analysis (HAZOP) was originally developed to identify both hazards and operability problems at chemical process plants, particularly for processes

using new technologies under development. The technique is also useful for analyzing the failure implications for existing processes as well.

A HAZOP requires an interdisciplinary team and an experienced team leader. The purpose of a HAZOP is to review a process or operation systematically to identify whether process deviations could lead to undesirable consequences. Reference 1 states that the technique can be used for continuous or batch processes and can be adapted to evaluate written procedures. It can be used at any stage in the life of a process. HAZOPs usually require a series of meetings in which the team systematically evaluates the impact of deviations using process drawings. The team leader uses a fixed set of guide words and applies them to process parameters at each point in the process. Guide words include "No," "More," "Less," "Part of," "As well as," "Reverse," and "Other than." Process parameters considered include flow, pressure, temperature, level, composition, pH, frequency, and voltage. As the team applies the guide words to each process step, they record each deviation with potential causes, consequences, existing or potential process safeguards and actions needed to prevent or mitigate the consequences, and/or the need for additional analysis to evaluate the impacts of the deviation or design the safeguards.

HAZOPs require more resources than simpler techniques such as FMEA. Ref 1 contains an extensive description and worked example of the HAZOP procedure.

Checklist Analysis

A checklist analysis is simply just that – it evaluates the process in question against existing guidelines using a series of checklists. This technique is most often used to evaluate a specific design, equipment or process for which an organization has a significant amount of experience. If a new project, for instance, is being performed using an existing system, checklists that cover accident prevention or best practices may already be in place for the existing system. This would make a checklist analysis on the new project easy to perform. If no appropriate checklist(s) exists, a range of project personnel of different backgrounds can develop it.

In general, once the system to be analyzed and its boundaries are defined, it is divided into subsystems or smaller, as appropriate. Then existing checklists are gathered for the various subsystems, and those that don't exist are developed. The questions put forth in the checklist are answered and, where needed, acted upon.

Ref 1 gives specific examples of the use of Checklist Analysis.

Fault Tree Analysis

Fault Tree Analysis is a deductive (top-down) method used for identification and analysis of conditions and factors that can result in the occurrence of a specific failure or undesirable event. The strength of the fault tree model is that it addresses multiple failures, events, and conditions. The analysis proceeds by constructing a graphical model of failure using a set of standardized logic symbols to represent the relationship of faults (failures, conditions, events) with the potential to result in the occurrence of the specific failure condition being analyzed. Fault tree analysis can address:

1. Independent, dependent, simultaneous, and common mode failures in systems and/or processes.
2. Effects of human errors, including operator and maintenance errors and external conditions.

The level of detail addressed in a fault tree is generally determined by the amount of data available, the desired level of resolution of the model, and the use of the fault tree (e.g., part of a larger study or not). Fault trees are generally developed and evaluated using available software packages, which can produce the fault tree diagram, lists of contributing events, and evaluate the likelihood of occurrence of the top event and contributing events.

Ref 1 discusses this option and also presents good examples of Fault Tree Analysis.

Event Tree Analysis

Event tree analysis is an inductive approach used to identify and quantify a set of possible outcomes. The analysis starts with an initiating event or initial condition and includes the identification of a set of success and failure events that are combined to produce various outcomes. The goal of an event tree analysis is to identify the spectrum and severity of possible outcomes and determine their likelihood. Event tree analysis produces a graphical representation of sequences of events leading to various outcomes.

An event tree analysis of an initial (initiating) event which must have successful safety system response to prevent an undesired end state, starts with the identification of all the safety systems that must function to prevent or mitigate undesired consequences. Then the systems are listed in order of expected operation and the success or failure of each system is then postulated. The effect of these successes or failures are identified and combined as individual sequences of events, sometimes referred to as accident sequences or scenarios. The result is a set of sequences representing combinations of failures and successes with varying consequences ranging from successful response to the maximum possible damage. Based on experience data and failure analysis of the events in each sequence, the likelihood of each sequence is determined. Event trees are generally developed and evaluated using available software packages, which can produce the event tree diagram, evaluate the likelihood of occurrence of each sequence, and group the sequences into groups of similar outcomes.

Ref 1 discusses this option and also presents good examples of Event Tree Analysis.

Probabilistic Risk Assessment

A Probabilistic Risk Assessment (PRA) is an organized process for answering the following three questions:

1. What can go wrong?
2. How likely is it to happen?
3. What are the consequences?

PRA methodology originated in the nuclear power and aerospace industries and has been adapted for use in the chemical industry, where this approach is called "Chemical Process Quantitative Risk Analysis" or CPQRA. A variety of analytical techniques are used in the performance of a CPQRA, depending on the scope and complexity of the problem to be addressed. The analysis steps and methods involved in performing a CPQRA are as follows.

1. Problem definition. Identification of study goals, choice of the risk measures to be used, selection of the depth of study to be performed, identification of the information resources required to perform the study.
2. System description. Compilation of the process/plant information (i.e. site location, weather data, process flow diagrams, piping and instrumentation diagrams, etc.) needed to perform the analysis.
3. Hazard identification. A critical step in CPQRA. Identifies the potential energy sources that can affect the system being analyzed and the potential hazardous material that can be released. Depending on the problem, approaches to be used to identify hazards include; a) data analysis, b) hazard identification check list, c) what-if analysis, d) hazard analysis techniques, e.g., HAZOP, FEMA, or PHA (Preliminary Hazard Analysis).
4. Incident enumeration and selection. Starts with an initial identification of all possible incidents without regard for importance or initiating event using processes such as data assessment or FMEA. Incidents are grouped by type and the most significant incidents from each type are determined and used to represent all identified incidents for the purpose of further analysis.
5. CPQRA model construction. Appropriate likelihood models and consequence models are selected and integrated into an overall model to produce and present risk estimates for the system under study. Likelihood models include use of historical data on events, fault trees, and/or event trees. Consequence analysis tools include fire, explosion, and direct (burns, impacts, etc.), health effects (lethal dose, long-term consequences) and material dispersion models.
6. Likelihood estimation. The methodology used to estimate the frequency or probability of the occurrence of an event or component failure can be obtained from historical data, or from developing and quantifying failure sequence models using fault tree and event tree analysis methods.
7. Consequence estimation. The methodology used to determine the potential for damage or injury from specific incidents includes direct (burns, impacts, etc.) and health effects (lethal dose, long-term consequences) models.
8. Risk estimation. The process of combining the consequences and likelihoods of all potential incidents to provide a measure of risk. The risks of all selected incidents are individually estimated and combined to give an overall measure of risk using techniques such as the development and quantification of damage states and plotting the risk in a graphical form (e.g. cumulative complementary distribution functions).
9. Utilization of risk estimates. Results from a risk analysis are used to make decisions based on the significance of events, failures, and/or conditions to the overall risk estimates.

Ref 2 provides a detailed description of the Chemical Process Quantitative Risk Analysis approaches and methodologies.

4.2 Risk Mitigation Plan

The purpose of a risk mitigation plan is to achieve acceptable risk. It is essentially an extension of the ISV analysis, as its construction usually follows that development. After identifying safety vulnerabilities, the project team will have a prioritized list of safety aspects that require action. A risk mitigation plan provides detailed design and operational modifications for each issue on that list. Typical aspects of a risk mitigation plan include a discussion of mitigation measures, a cost effectiveness analysis, and an implementation strategy.

Mitigation plans are expected for events that could reasonably result in an unintended release of hazardous material or in injury to people. A risk mitigation plan assesses the scenarios and identified hazards from the safety assessment. The plan should determine the likelihood of occurrence, which could be expressed in frequency of occurrence, and the severity of consequence. It should consider the cause(s) of the scenario (or initiating event[s]) and the hazardous material or energy released as a result of the scenario. During this phase of the analysis, focus should be on those hazards that are of greatest concern.

Risk ranking is one analysis tool for risk mitigation. Each hazard can be plotted on a frequency/consequence (risk) matrix, which would indicate its level of risk – high, moderate, low, or negligible. For example, if a potential hazard's frequency is unlikely, and its consequence level is high, it would be a high risk. If a risk ranking tool is used, the criteria for assigning frequency and consequence categories should be included. The uncertainty of assigning events to these bin categories should also be addressed. Risk ranking can consider a base case design with any provided prevention and mitigation devices to determine if additional facilities are warranted. The following categories could be used for organizing and analyzing data:

- Event number
- Event category
- Postulated event description
- Causes
- Preventive features
- Frequency level
- Mitigative features
- Consequences
- Risk bin number

The consequences category should always include damage to a structure due to overpressure, or a secondary fire where the hydrogen leak is ignited. Consideration should also be given to the risk of an equipment/facility fire started elsewhere that endangers facilities and personnel where hydrogen is being used.

Examples of a risk-ranking matrix and frequency and consequence criteria tables are available in HyApproval Deliverables D4.3, D4.5, D4.11 & D4.12.

As already mentioned, risk mitigation also includes safety performance monitoring, management of change, safety documentation collection and maintenance, standard operating procedures development and use, employee training, and equipment maintenance. Although descriptions of these have already been given, some additional information is warranted for some of these items, and this material follows.

Safety Performance Measurement and Management of Change Reviews

A good measure of a safe HRS infrastructure development is its acceptance by regulatory authorities, and an important step is to quantify risks. A thorough safety plan will serve as a basis on which the risks associated with a technology may be measured. The plan needs to include a description of how safety performance will be measured and monitored, while ensuring that the ISV analysis is updated regularly as operating data becomes available.

The method to be used for reviewing the safety implications of any potential changes to project materials, processes, equipment, and operating/repair procedures should be stated along with a management commitment to implement the MOC procedure (see 3.2A). In addition, the contractor should establish and implement written procedures to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures

Employee Training

It is crucial to provide hydrogen safety training for all project personnel responsible for handling equipment containing hydrogen. The training program/procedures should be described and a management commitment to implement the procedure should be documented. An employee training program might have steps similar to these:

1. Each employee presently involved in operating a process, and each employee before being involved in operating a newly assigned process, is trained in an overview of the process and in the operating procedures. The training includes emphasis on the specific safety and health hazards, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.
2. In lieu of initial training for those employees already involved in operating a process, the contractor certifies in writing that the employee has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities as specified in the operating procedures.
3. Refresher training is provided to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures of the process. The contractor, in consultation with the employees involved in operating the process, determines the appropriate frequency of refresher training.
4. Training documentation: The contractor ascertains that each employee involved in

operating a process has received and understood the training. The contractor keeps a record, which contains the identity of the employee, the date of training, and the means used to verify that the employee understood the training.

Procedures to Ensure Equipment Integrity

Equipment integrity maintenance might take a form similar to the following:

1. The contractor/HRS infrastructure supplier establishes and implements written procedures to maintain the on-going integrity of process equipment, including calibration procedures for safety-related equipment.
2. The contractor trains each employee involved in maintaining process equipment to ensure that the employee can perform the job tasks in a safe manner. An overview of the process and its hazards and the operating procedures applicable to the employee's job tasks are provided.
3. The frequency of inspections and tests of process equipment is consistent with applicable manufacturers' recommendations and best engineering practices, and more frequently if determined to be necessary by prior operating experience.
4. The contractor documents each calibration, inspection and test, including any hydrotests or leak tests, performed on process equipment. The documentation identifies the date of the inspection or test, the name of the person who performed the inspection or test, the serial number or other identifier of the equipment on which the inspection or test was performed, a description of the inspection or test performed, and the results of the inspection or test.

4.3 Communications Plan

As noted on Page 5, safety event reporting is one element of a comprehensive and effective communications plan. The primary purpose of safety event reporting is the prevention of incidents. By learning about the likelihood, severity, causal factors, setting and relevant circumstances regarding hydrogen safety events, one is better equipped to prevent similar incidents in the future and at other facilities. It is especially desired to learn from past experience to prevent the occurrence of events that are more severe (using "lesser" events to prevent worse ones). This philosophy requires a great deal of information sharing as openly and thoroughly as possible. Project managers, learning about and reporting a safety event, can help facilitate the prevention of other events.

Both incidents and near-misses are reportable events for projects within the EU CUTE (now completed) and HyFLEET:CUTE programmes and are described as follows:

- An **INCIDENT** is an event that results in:
  - a lost-time accident and/or injury to personnel,
  - damage and/or unplanned downtime for project equipment, facilities or property,
  - impact to the public or environment,
  - any hydrogen release that unintentionally ignites or is sufficient to sustain a flame if ignited,

  - any hydrogen release which accumulates above the lower flammability limits within an enclosed space.
- A **NEAR-MISS** is an event that under slightly different circumstances could have become an incident.

The above list is not inclusive of all possible and reportable events, but is indicative of incidents that should be reported. HRS infrastructure suppliers and operators are encouraged to report safety and hydrogen release information they believe will have learning benefits for others.

5. References

1. *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples,* Center for Chemical Process Safety, American Institute of Chemical Engineers, 1992.

2. *Guidelines for Chemical Process Quantitative Risk Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2000.

3. For examples of Hazard Identification Tables and Risk ranking Matrixes*: refer to HyApproval Deliverables D4.3, D4.5, D4.11 & D4.12.*

4. EU CUTE Project Deliverable D3 (Quality and Safety Methodology, dated 20/3/2006)
(Note: This Document is presently restricted to EU CUTE Project partners until approved and released for public access by the EU)

Appendix A – Safety Plan Approval Form

Project Name / Number: _____

Project Title: _____

Organization: _____

Safety Plan submitted by: _____

Safety plan prepared by: (**EXAMPLE:** Primary Author / Project Initiator [PI])

Name
Title
Department/Division

Safety plan reviewed by: (**EXAMPLE:** Next Level Management Above PI)

Name
Title
Department/Division

Safety plan approved by: (**EXAMPLE:** Organization's Safety Representative)

Name
Title
Department/Division

Note: Additional signature lines should be added as required by the applicable organization.