# System Description and Hazard Identification:

# A Process for Design and Manufacturing Organizations

Alan J. Stolzer, Ph.D.

Embry-Riddle Aeronautical University

# TABLE OF CONTENTS

## 1. PURPOSE

a) This appendix:

i) Presents a procedure for a Design and/or Manufacturer (D&M) firm to follow to create a system description of its organization.

ii) Should be used after and in concert with the Design and Manufacturing Safety Management (SMS) Pilot Project Guide which fully explains SMS for D&Ms.

iii) Shows how the system description plays a key part in a company's Safety Management System (SMS), supporting other efforts such as safety policy, risk management, safety assurance, and safety promotion.

iv) Explains that, while an organization may employ existing management systems and/or other hazard and risk tools[1], the intent of a system description is, in part, to identify the existence and placement of these analysis methods within the organization or the absence thereof.

b) This appendix is not mandatory and does not constitute regulation. There are a variety of ways that an organization can approach SMS. This appendix is intended to provide an organization with one possible alternative for creating a system description that can facilitate hazard identification.

## 2. APPLICABILITY

This appendix applies to companies that design and/or manufacture products for aviation, from large systems such as airliners, to smaller systems such as engines and propellers, to supporting parts such as batteries, starters, and fittings. While the text refers to "Design *and* Manufacturer" (D&M) companies, this is done for brevity. Whenever D&M is referred to, the reader should understand "design and/or manufacturer."

For those instances where crossover designs exist (i.e., where one organization designs and another manufactures), the procedure will guide the user through such identification. The term D&M is meant to include this type of arrangement.

## 3. RELATED READING MATERIAL

The following references, current editions, may be of value to users of this appendix, as they develop their system descriptions:

- International Civil Aviation Organization (ICAO) Document 9859, ICAO Safety Management Manual (SMM, Second Edition, 2009)

[1] For example, Failure Modes and Effects Analysis (FMEA) or Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis.

- Advisory Circular (AC) 120-92A, Safety Management Systems for Aviation Service Providers[2]

- FAA Order 8000.369, Safety Management System Guidance

- FAA Order VS 8000.367, Aviation Safety (AVS) Safety Management System Requirements

Hazard Identification References


- Bahr, N. J. (1997). *System safety engineering and risk assessment: A practical approach*. New York: Taylor & Francis

- Ericson, C. A. (2005). *Hazard analysis techniques for system safety*. Hoboken, NJ: John Wiley & Sons

- Manuele, F. A. (2003). *On the practice of safety, 3rd edn*. Hoboken, NJ: John Wiley & Sons

- Mikulak, R. J., McDermott, R., Beauregard, M. (2008). *The basics of FMEA, 2nd edn.* Unknown: Productivity Press.

- Petersen, D. (2003). *Techniques of safety management: A systems approach, 4th edn.* Des Plaines, IL: American Society of Engineers

- Roland, H. E., & Moriarty, B. (1990). *System safety engineering and management, 2nd edn.* Hoboken, NJ: John Wiley & Sons

- Stephenson, J. (1991). System safety 2000: A practical guide for planning, managing, and conducting systems safety programs. Hoboken, NJ: John Wiley & Sons

- Stolzer, A. J., Halford, C. D., & Goglia, J. J. (2008). *Safety management systems in aviation*. Burlington, VT: Ashgate Publishing


## 4. BACKGROUND

The user of this procedure should be familiar with the role that SMS will play in all aviation enterprises. The recommended reading material, particularly the ICAO and FAA documents, provides this background.

[2] Although this Advisory Circular was created for operators and maintenance service providers, the fundamental SMS principles are relevant to D&M.

a) A system description can be thought of as an account of organizational structures, procedures and processes, people, equipment, and facilities used to accomplish the organization's mission.

   i) The process used to identify hazards must consider all components of the system design; thus, it is necessary to begin with a system description that takes into account those components and their interactions.

   ii) While individual parts or functions of the organization may have descriptions and hazard elements, the intent of this description is to bring together those elements into an overarching view of the system as a whole; thereby enabling overall system analysis.

   iii) There is no specified format for a system description, but it should be thoroughly and effectively documented.

b) D&M companies differ from other aviation industry businesses in that they

   i) Must deal with product lifecycles, such as requirements, design, testing and certification, production, support, and product retirement.

   ii) Have to manage the safety of their fielded product, as well as the processes which create the product.

   iii) Generally have a quality management system in place, such as AS9100[3], that may simplify the development of a system description, the identification of hazards, and the implementation of SMS.

c) A system description provides a detailed view of an organization sufficient to relate hazards to parts of the description. The system description provides the foundation upon which proactive hazard identification can occur.

d) The procedure defined in this document is intended to guide an organization through the process of creating a system description to facilitate proactive hazard identification. The focus of the present procedure is on the development of a system description. The user should refer to other resources for specific techniques regarding hazard identification.

e) The desired outcomes of this procedure are:

   i) To develop an organization's understanding of a system description.

   ii) To create a system description for your organization; and

[3] AS9100 is a family of standards contains all of the requirements of ISO 9001:2008, the global standard for quality management systems, in addition to numerous additional requirements specific to the aerospace industry.

iii) To develop an initial set of high level hazards for further analysis.

## 5. PROCEDURE OVERVIEW

The system description procedure consists of the steps shown in Figure 1. Each step of the procedure is expanded on in this appendix.

a) The procedure is most effective when carried out in a group environment. The core constituents of the group should be upper management, which controls the organization's resources and draws upon other staff members to develop the system description details defined by each step.

b) The system description procedure will touch on many aspects of an organization's operations and, as such, may generate large amounts of information. The suggested format to collect the information is to use wallboards to post notes of information discovered in each step, or electronic aids such as mind mapping software. The system description effort will require a significant amount of time to assemble and compile the raw data, and involve a number of individuals. While certain departments of the organization's organization may be excluded from the process, such exclusions must be done deliberately and with caution. The intent of a system description is to include all facets of an organization, at the appropriate level. For example, while janitorial may be excluded from the system description, what if janitorial at night can disrupt calibration of manufacturing equipment? Consider the ramification of such exclusions.

c) Throughout this procedure, the user should remain cognizant of the end goal, which is to identify hazards that may exist in the organization. Although it is advisable to not focus excessively on hazard identification during the development of the system description, the user may find that some hazards become apparent; these should be recorded. A hazard numbering scheme should be developed and used throughout the procedure.

d) Upper management must create an environment for success. Sufficient time must be allocated to procedure execution. To preclude the rank and file perceiving this as unimportant, it is vital that management set expectations regarding the procedure, including strategies to avoid fatigue and conflict during its execution.

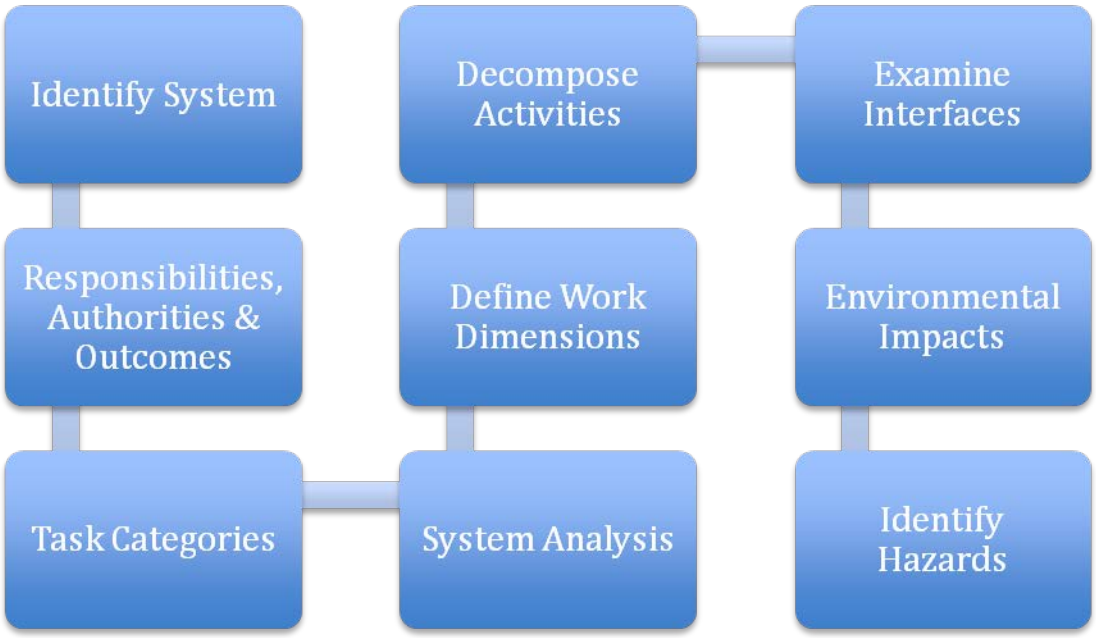
e) Most steps of the procedure will ask the organization to examine itself from the perspective of *product lifecycle* as well as different *domains* of an organization:

i) The *product lifecycle* refers to stages of product, such as requirements, design, testing, certification, production, delivery, support, and retirement.

ii) The *domain* is less obvious but equally important in discovering details at each step in the process. Domains refer to *Organization, Design, Process,* and *Product.* Generally, the *organizational* domain consists of such areas as

accounting, human resources, marketing departments, etc. The *Design* domain refers to the methods an organization uses to executes its designs. The *Process* domain refers to the methods an organization uses to make its products such as material selection, tooling, shop procedures, etc. The *Product* domain is the product you sell. For design-only houses where no parts manufacture or assembly occurs, this "product" is usually an FAA approved design.

**FIGURE 1. SYSTEM DESCRIPTION PROCEDURE OVERVIEW**




## 6. PROCEDURE

### a) IDENTIFY SYSTEM

This step consists of broadly identifying what your organization does. Figure 2 shows a graphical way to identify a system in terms of the inputs to the organization, the outputs - what is produced, the resources required, the controls guiding the processes, and in the center, the activities that make up the organization. Subsequent steps in the procedure expand upon this first step.

Responding to the following points, organized by *domain*, will aid the user with this step. *Note*: these are samples of questions that may be asked. Some will not be relevant for every organization; simply disregard. Add other questions/issues as appropriate.

i) *Organizational Domain.*

- What is the type of organization – design? Manufacturer? Both?
- Describe the resources used by the organization, how many employees? What type of employee skills? Who are the customers? What facilities does the organization use? Who are the suppliers? What information systems are used in the organization?
- What reputation does the organization hold in its product sector? How important is reputation? Is there a reputable product base?

*ii) Design Domain*

- What methods are used to identify hazards?
- Describe existing design methods.
- What are the regulatory constraints?
- How is design documentation control performed?
- How is organization knowledge maintained over time, i.e., artifacts of prior designs or methods?

iii) *Process Domain.*

- What methods are used to identify hazards?
- Describe existing manufacturing methods.
- What are the regulatory constraints?
- How is documentation control performed?
- How is organization knowledge maintained over time, i.e., artifacts of prior designs or prior manufacturing methods?
- How are product defects tracked, both during production and in service? What are the defect rates? Are defect rates known? Are they reliable?

iv) *Product System.*

- What method is used to identify requirements?
- What methods are used to identify hazards that the product will encounter in service? How are such hazards documented and maintained?

- What method is used to identify design requirements? How are materials selected? What environmental factors is the product subject to? How are strength requirements created?

- What design standards exist? What are industry practices for the products? Are any non-standard industry practices used? How were design or manufacturing standards established?

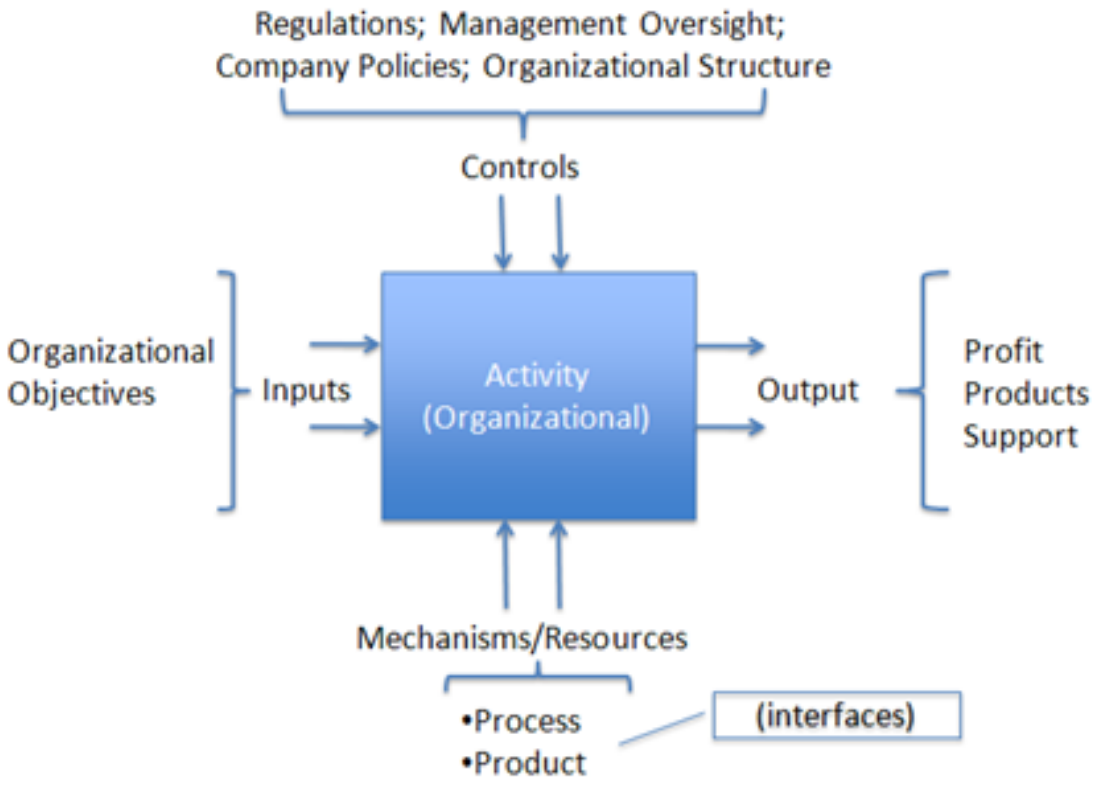
- What methods are used to identify needed toolings?

- How are total in service times for all sold products known or estimated? How many of the organization products are still in service?

- What are the testing methods to verify the design? Each manufactured item?

- What quality control and consistency methods are used? Are they effective? What measures support the knowledge?

**FIGURE 2. IDENTIFY SYSTEM GRAPHICAL PRESENTATION**



b) **AUTHORITIES, RESPONSIBILITIES, AND OUTCOMES.**

For the organizational, process, and product domains to be effective, there must be a definition of responsibilities, authorities, and outcomes. That is, *authority* refers to a person or group that controls the overall system and governs change of the system, whereas the *responsible* person or group controls the execution of the system. The authority and responsibility roles exist to produce desired *outcomes*. This step identifies the authorities, responsibilities, and outcomes.

i) *Organizational Domain.*

- What is the organizational chart of the organization? Is it up to date?
- What job descriptions exist for each employee? Are they accurate?
- Do all persons know their areas of authority and responsibility and what outcome is expected of them?
- How are individual outcomes measured?
- What is the nature of the authority reporting chain? What level of independence exists as opposed to hierarchal reporting structures?

ii) *Design Domain*

- Who has authority over the design process? *Note:* This is similar to the organizational question, but it looks outward to the personnel, rather than the prior step that looked from people towards outcomes.
- Similarly, who is responsible for each step in the design process?

iii) *Process Domain.*

- Who has authority for each process in the organization? *Note:* This is similar to the organizational question, but it looks at the process outward to the personnel, rather than the prior step that looked from people towards processes.
- Similarly, who is responsible for each process in the organization?
- Do the authorities and responsibilities change for different lifecycles of the process supporting a product? For example is the same person or group responsible for manufacturing as is responsible for customer support of in service products?
- In terms of outcomes, what processes exist for: marketing, design, production, installation, operation, support, retirement?

iv) *Product Domain.*

- Who has authority over each product?
- Who has responsibility over each product?
- Do the authorities and responsibilities change depending on the product lifecycle, i.e., are the same people responsible for the product during design, production, and in service?

c) **TASK CATEGORIES**.

This step adds more detail to the emerging system description of the organization. The activities that make up an organization are looked at from four perspectives of *operations, administration, supervisory,* and *resources.* While these four perspectives can be considered in the organization, process, and product domains, it is simpler to address the perspectives independent of domains.

i) *Operations Perspective*

- What types of tasks are performed to define the requirements of a product? What types of tasks are performed in designing a product? What types of tasks are performed in manufacturing a product? In delivery/installation of a product? In support of a product? In overhaul or retirement of a product?
- What tasks go into supporting the products and processes, such as accounting, human resources, information technology, and employee training?
- What tasks support business continuity of facilities? Information systems?

ii) *Administrative Perspective*

- What tasks are necessary to maintain regulatory compliance? What tasks to maintain certifications and/or licenses?
- What legal tasks are necessary to support new products? Existing products? Retired products?
- What tasks are necessary for employee time keeping? Lost work injury reporting?
- What tasks define budgeting?

iii) *Supervisory Perspective*

- What tasks are performed related to supervision, such as employee job reviews, team-building exercises?
- What supports a safety culture, such as a just culture[4]? Is reporting a potential design, process, or product flaw encouraged? If so, how?
- What tasks identify how safety/quality is measured?
- What tasks define how supervisors achieve regulatory compliance?

iv) *Resource Perspective*

- What tasks are used to define the organization's assets? Credit? Liabilities?
- What tasks are involved in maintaining the accounting systems?
- What tasks are involved in maintaining the information technology systems?
- What tasks are used to manage vendors and suppliers?
- What tasks are used to manage supply inventory?
- What tasks manage orders for future organization products?
- What tasks insure a sufficient number and quality of employees? What tasks insure adequate facilities? What tasks insure adequate tools?

*Note: The system description emerging at this point should have a growing amount of detail. The process of creating the system description may have already yielded benefits to the organization in terms of identifying ill-defined areas. Further, the system description process thus far has likely involved many people in the organization contributing needed details.*

d) **SYSTEM ANALYSIS**.

This system analysis section seeks to identify factors that affect the performance of the system. This is done using an acronym known as SHEL – software, hardware, environment, liveware (people). As was done with task categories, the organization, process, and product domains will not be specifically delineated for sake of simplicity.

[4] A just culture means an environment where people are encouraged to report mistakes without fear of reprisal.

i) Software

- What organizational policies and procedures exist in the organization? How are they maintained? How are they communicated?
- What templates are used to guide recurring processes?
- What supplier agreements exist?
- What procedures are used to define requirements for new products or product variants? To perform hazard/risk analysis on new product designs?
- What forms of configuration management are used to control manufacturing processes? To control information technology systems?
- What procedures are used to control versions of product manuals?
- What procedures are used to control design specifications?

ii) *Hardware*

- What elements make up the information technology support systems of the organization?
- What facilities are available to the organization and what are the capabilities, i.e., square footage, electrical capacity, size capacity, hazardous material handling?
- What manufacturing tools are required to create products? What spares support the necessary manufacturing tools?
- What raw materials are needed to create the organization's products?
- What defines the interfaces of an organization-produced product with other parts of the system on which it is installed (or operates)?

iii) *Environment*

- Within the organization, how is a just culture maintained—that is, how are employees encouraged to report deficiencies?
- Describe the safety council within your organization.
- How do the legal/litigation aspects of the organization relate or conflict with safety objectives?
- How are workplace rules documented?

- What is the regulatory environment of the organization and its products?
- How is the operating environment wherein the organization products operate factored into design, production, and service?
- How does the economy affect the demand for products?

iv) *Liveware*

- How does the organization attract qualified employees?
- What methods are used to insure there is sufficient staffing for the organization?
- How are personnel trained to do their jobs? How are they measured in job performance?
- Who are the people who use the products made by the organization?
- Who maintains the products produced by the organization when the product is in service?
- If applicable, who overhauls/refurbishes products at the end of their lifecycle?

e) **DEFINE WORK DIMENSIONS.**

Work dimensions acknowledge the reality that companies exist to make a profit. The work dimensions necessary to make a profit include quality, service, pricing, delivery times, safety, reputation, and others. In some cases, these business objectives promote safety, in other cases the business goals detract from safety.

i) *Organizational Domain.*

- How does the organization mitigate against product liability claims?
- How are production rates predicted? How often does production lag behind promised delivery rates?
- What organization procedures are in place to maintain regulatory compliance and reporting?

ii) *Design Domain.*

- What methods are used to develop measures of production quality?
- What methods are used to measure customer satisfaction?

iii) *Process Domain.*

- What methods are used to develop measures of production quality?
- What methods are used to measure customer satisfaction?

iv) *Product Domain.*

- How are safety objectives of a product determined?
- How are customer prices and profit margins determined?
- How are service issues of in service products determined?
- How are the environmental issues of organization products determined, i.e., for batteries, how are they disposed; for de-icing fluid, how are effects to the environment considered?

f) **DECOMPOSE ACTIVITIES.**

This step allows for a detailed description of activities within the organization. Clearly, this list could go on to a level of detail that would be counterproductive. The objective in this step is to create an appropriately detailed outline of activities to facilitate subsequent, deeper analyses.

i) *Organizational Domain.*

- What activities are used to maintain the organizational chart?
- What activities are performed to manage the following areas: regulatory compliance, organization assets, information technology resources, facilities, suppliers, intellectual property, and product liability?
- What activities are involved in organization information systems to preserve historical records of the organization?

ii) *Design Domain.*

- What activities are used to solicit and develop product design requirements?
- What activities transform requirements into technical designs and how are the designs validated against requirements?
- How activities are used to develop and to measure design quality?

iii) *Process Domain.*

- What activities are used to solicit and develop product requirements?
- How are process measures developed to measure quality?
- What activities make up manufacturing of products?
- What activities are necessary to deliver products?
- What activities support in service products?
- What activities measure the number of active, in service organization products?

iv) *Product Domain.*

- What activities are used to assess how products are actually used and maintained in service?
- What activities are anticipated to maintain products in service?
- What activities are performed to train users and maintainers of the product?
- What activities occur in response to failures of the product, i.e., accident and incident investigation?

g) **EXAMINE INTERFACES**.

Clearly the activities of an organization are related to each other. This step considers the *interfaces* between activities both *within* and *external* to the organization. In addition to considering interfaces of activities, interfaces of aspects of the SHEL step should also be considered.

i) *Organizational Domain.*

- How do actions of the safety council impact policy, procedures, and processes?
- What labor contracts exist? How do labor contracts affect work rules?
- How are non-employee personnel (i.e., vendors, contractors) accounted for in the organization?
- How do financial goals relate to supplier selection?

- How do regulatory requirements affect anonymous reporting and a just culture? Likewise, how do litigation concerns affect anonymous reporting and a just culture?

- If applicable, how do suppliers of products (or labor) affect organization objectives, such as a just culture as well as quality standards?

ii) *Design Domain.*

- What product lifecycle data such as service needs, failures, and defects get fed back to the design process?

- How are in-service issues communicated to define design requirements?

- How are these requirements verified in resultant designs?

iii) *Process Domain.*

- How do lifecycles of production interface? That is, how are design requirements translated into manufacturing methods? How are design and manufacturing methods used to correct defective and/or broken in service products?

- How are in service issues communicated back to design requirements?

- How are manufacturing personnel measured as doing their jobs according to policies created by the organization? That is, how well aligned is shop floor reality to process design?

iv) *Product Domain.*

- How does the organization measure customer usage of its products in service against the planned in service usage techniques?

- How are regulatory changes adopted into design changes? How are regulatory changes applied to in service products (including service bulletins, airworthiness directives, etc.)?

h) **ENVIRONMENTAL IMPACTS**.

While the prior step considered interfaces in general, this step looks specifically at how the external environment impacts the functioning of the organization as a system.

i) *Organizational Domain.*

- What business continuity plans are in place for manufacturing or office space disasters (i.e., if the manufacturing facility burned down in a fire)?

- What business continuity is in place for information systems?
- How does the organization keep informed of regulatory changes?

ii) *Process Domain.*

- How are design requirement changes managed?

iii) *Process Domain.*

- How are product requirement changes managed?
- How are manufacturing methods changes managed?
- What is done to protect against dependence on a key, manufacturing tool (or software) becoming obsolete?

iv) *Product Domain.*

- How are changing conditions of the environment the products operate in made known to the organization?
- How are supply chain issues needed to manufacture or maintain products assessed?
- How are the organization's products integrated with their host or parallel systems (e.g., if the product is a tire, how is it known it works properly on the landing gear of an Acme 'Rocket' plane)?
- What impact is there on a product's in-service use if the product is retired or upgraded to a newer version?
- What impact is there on any applicable backward compatibility if a product is retired or upgraded to newer version?

## 7. SUMMARY

Performing the eight steps (a-h above) should have created a wealth of notes, artifacts, and raw data. If the process was done in a group environment, there were possibly disagreements that exposed ambiguities not previously known to all parties. The notes taken to this point should be preserved and a system description written that summarizes the organization as a system. Two example work products of this system description procedure for a small Parts Manufacturer Approval (PMA) house that makes rotor shafts and a large multi-national organization are provided as Attachments I and II, respectively.

## 8. HAZARD IDENTIFICATION

The development of a system description is a prerequisite to an effective, proactive hazard identification process in an organization. This AC closes both by defining a hazard and encouraging the reader to make a list of high-level hazards by providing a list of generic hazard categories.

a) The D&M SMS Pilot Project Guide defines a hazard as a "Condition, occurrence, or circumstance that could lead to or contribute to an undesired event. Sometimes termed "threat". An "undesired event" can be but is not limited to: injury, illness, or death; damage to or loss of a system, equipment, or property; or detriment to the environment."

b) *Organizational Domain Generic Hazards.*

i) Poor definition of responsibilities and authority

ii) Intellectual property compromise

iii) Product liability

iv) Undetected change

v) Regulatory violation

vi) Financial loss

c) *Process Domain Generic Hazards.*

i) Changes to methods or procedures

ii) Incomplete process definitions

iii) Changes to supply chain

iv) Manufacturing hazards to personnel (i.e., OSHA type hazards)

d) *Product Domain Generic Hazards*

i) Incorrect product requirements

ii) Product manufacturing defects

iii) Unanticipated failure modes

iv) Products not used or maintained as designed

## ATTACHMENT I

### Fictitious Example – Small Rotor Shaft Company

The purpose of this section is to show a practical application of the system description process for a small company. This fictitious example considers a small, five-person rotor shaft company, primarily built around a machine shop and a few core products. As the reader progresses through the example, reference should be made to the noted Procedural Document.

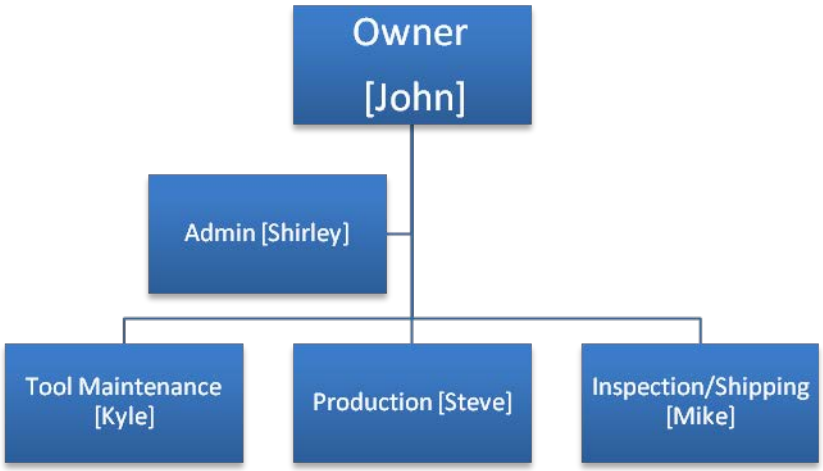
Throughout this narrative, certain details may be omitted to express the essence of the process, however, the reader should keep in mind that the process is necessarily an interactive, group exercise. Ideally the group will have core constituents and invite various members of the organization in to help expand the depth of the expertise at certain stages.

As the system identification process is executed, watch for hazard identification opportunities as the Procedural Document recommends. For any hazard noted in the system description, have a method to add it to the stack of hazards for later consideration. That is, while the process is described linearly, it is fine to jump ahead and move back throughout the process. In this presentation, whenever a discovered hazard is identified it will be noted as follows: {HAZ: Defects in supply chain}.

### Identify System

The company is looked at from three perspectives: organizational, processes and products.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| The system identified is essentially a machine shop producing rotor shafts under contract to helicopter manufacturers | {HAZ: Machine shop does not know details about design or operational conditions of shafts} |
| All management are also hands-on workers | {HAZ: Conflicting priorities} |
| Process | |
| Same processes used for many years, as specified by the helicopter company | |
| Inspections done by our shop are repeated by the helicopter company upon product delivery | {HAZ: May depend on helicopter company to find problems} |
| Product | |
| Only new rotor shafts are made, no overhauls. Products limited to what machine shop tooling can handle. | |




**Responsibilities, Authorities and Outcomes**

The organization chart used to identify the system is expanded upon to show authority and responsibility within the company.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| President (John) is everyone's boss | {HAZ: May lead to personality driven processes} |
| Process | |
| Authority for rotor shaft inspections lie with Mike. He reports problems to John, who decides on corrections. Shirley has responsibility to talk to helicopter company for orders and shipping notification. | |
| Product | |
| Outcome of a rotor shaft is a mid-process product, which is refined, and inspected by helicopter company before installation. Rotor shafts are expected to last 2,000 hours. | {HAZ: Failures may be hard to identify who introduced flaw} |

## Task Categories

Task categories are looked at from four areas: operational, administrative, supervisory, and resources. The product and process dimensions are looked at only on the operational area across life cycle dimensions. Organizationally, the operational and supervisory perspectives were adequately described by the *Responsibilities, Authorities and Outcomes* step.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| *Administrative* functions are handled by Shirley. She does payroll, a/r, a/p, subscription renewals, etc. | {HAZ: Shirley is sick or on vacation, things may get missed} |
| Kyle handles computer *resources* and fixes computers. Backups done by online backup service. | {HAZ: Many paper processes and documentation, could be lost if building destroyed} |
| John ensures there are adequate *resources* including cash flow for payroll, building leases, utilities contracts and salary levels. | {HAZ: Informal process to project adequate cash flow} |
| Process | |
| Company is only concerned with *production*. Biggest issue is to supplier of raw steel and lead times of 60 days on orders. | {HAZ: No alternative raw material provider} |
| *Delivery* is done by Mike, who needs to crate shaft and get it on truck for delivery | {HAZ: Shaft can be damaged during delivery} |
| Product | |
| Once helicopter company accepts rotor shaft, our firm has no further obligations. Our contract is written such that the helicopter company takes on full responsibility for the product after delivery | |

## System Analysis

Using the SHEL – software, hardware, environment and liveware – heuristic, the system is analyzed along its organizational, process and product dimensions.

| | Item | Hazard (if identified) |
|---|---|---|
| Organizational | | |
| S | Shirley manages people and benefits plans. | |
| H | Kyle maintains computers and tools on shop floor. | {HAZ: If lathes change, a new certification is required from helicopter company} |
| E | Problems in production are reported to John | {HAZ: With so few people, cannot have anonymity} |
| L | Job functions are closely aligned with each person (John, Shirley, Kyle, Steve, Mike) | {HAZ: Personality driven process, if people were to leave, hard to replace} |
| Process | | |
| S | Blueprints and spec sheets for shafts stored in fireproof file cabinet in office | {HAZ: Original documents guiding production not reviewed often, could lead to practical drift} |
| H | Shop floor, lathes, and associated tools in working order is critical | |
| E | Clean workplace, adequate ventilation, and safety control devices (e.g., hardhats, safety goggles) | |
| L | Experience of Steve on floor is critical, along with inspections by Mike. | |
| Product | | |
| S | FAA form XXX must accompany each delivered shaft | {HAZ: Form may become substitute for actual inspection and quality} |
| H | Produced rotor shaft | |
| E | Our company builds shafts to helicopter company specifications – we are not in the loop on actual environment. | {HAZ: Our knowledge and experience is not fully utilized to see "big picture" problems} |
| L | Helicopter inspectors who receive shafts from us | |

## Side Bar – Process Note

*The reader should keep in mind throughout this process the end goal – the end goal is a hazard analysis. Each analysis point provides an opportunity to identify a hazard, as has been exemplified through the introduction of the* ***{HAZ: note}*** *notation. The organization as whole makes up the safety management system, thus the importance of the analysis being conducted.*

## Work Dimensions

The next step in the system identification process is to look at work dimensions. One way to do so is to organize work dimensions as safety compatible and counter to safety (in the associated table, "✓" is for compatible, "✗" is for counter).

| | Item | Hazard (if identified) |
|---|---|---|
| Organizational | | |

| | Item | Hazard (if identified) |
|---|---|---|
| ✓ | Helicopter company annual inspections of facilities and processes for contract renewal | |
| × | Minimal workforce for economy limits backup employees | |
| | Process | |
| ✓ | Quality measures used in the production (by Mike) used to accept or reject shaft | {HAZ: Quality measures may not have regular review} |
| × | Shafts rejected by Mike cost company money | |
| | Product | |
| ✓ | Minimum defects in delivery | |
| × | Desire to stay with one raw material provider | |

**Decompose Activities**

The work defined thus far has outlined a system. This step draws out specific activities that make up the broader system. This step can be a useful review of the prior steps and will often yield additions to prior steps in the process.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| John reviews contracts, production rates, defect reports and supervises all employees. | |
| Shirley processes payroll, a/r, a/p, answers phone calls, maintains FAA required records | |
| Process | |
| Kyle maintains shop tools, John and Shirley's computers | |
| Steve mounts raw steel on lathe, lathes shafts, cleans/polishes | |
| Mike inspects shafts, fills out FAA form XXX, provides copies to Shirley along with shipping information, boxes shaft and arranged truck shipping. | |
| Product | |
| Helicopter company receives and signs off on product | |
| John is notified, via Shirley, if any rejects by Helicopter company | |

**Examine Interfaces**

Like decomposing activities, interfaces provide another retrospective opportunity.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| John works with helicopter companies, gets accounting information from Shirley, oversees production quality received from Mike | |
| Shirley gets records of shipping and production form FAA XXX from Mike; Kyle fixes computer issues for Shirley and makes sure online backups work | |
| Kyle fixes Shirley's computer when it breaks, advises John when tooling is in need of replacement. | |
| Process and Product | |

| Item | Hazard (if identified) |
|---|---|
| Steve advises Kyle when shop equipment needs repair or calibration; advises Mike when a shaft is ready for inspection. | |
| Mike works with shipping company to send shafts; crate company to keep supply of crates and shipping materials; provides Shirley with records of shipping. | |

**Environmental Impacts**

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| Each employee has irreplaceable knowledge with little duplication of skill | |
| Process | |
| Location of filing cabinet with original designs (blueprints) is far from shop floor, so difficult to inspect | {HAZ: Practical drift in production} |
| Designs don't change often, but when they do it takes a while to get up to speed | |
| Product | |
| Shaft failure in operations is a catastrophic event | {HAZ: Chain of authority through helicopter company may obscure how critical our role is} |

## Hazard Identification

The system analysis should have spawned numerous opportunities to identify hazards in the system, again broken down by organization, process and product. Within this example, the process produced many hazards, but still only a subset of what an actual execution of the process would yield. The list that follows is only a small fraction of the total hazards that could be identified from the system analysis. Furthermore, it includes a summary of the hazard items identified as well as new hazards this step itself introduces.

| Organizational |
|---|
| Machine shop does not know design or operational details of shaft usage |
| Small company leads to conflicting priorities of Management (John) |
| Personality driven processes |
| When Shirley is sick or on vacation, things may get missed |
| Paper documentation all in one place |
| Informal process to project adequate cash flow |
| Process |
| Helicopter company is relied upon to ultimately identify defects |
| No alternative supplier of raw materials |
| With only five people in company, anonymity of problem reporting difficult |
| Quality measures may not have regular review (by John) |
| Original documents (blueprints) guiding production not reviewed often |
| Product |
| Failures in shaft may be hard to identify in our company or helicopter company |
| Shaft damage during delivery |
| FAA Form XXX may be substitute for actual intent – quality, defect free shaft |
| Full conditions of shaft unknown to our company – we only produce to a given specification |

### Conclusion

The system description of the company as well as hazard identification is the foundation of a safety management system. It should become clear by the time the analysis is executed that the system analysis herein is a *macro* view of the company. What follows the macro view are numerous *micro* views of many supporting processes: a similar analysis and hazard identification procedure can and should be executed for each process within the company.

Of course for each hazard the associated risks must be drawn out and an assessment made of the likelihood and severity of such risks. For those risks deemed unacceptable, controls must be put in place and then assurance processes put in place to verify the controls behave as expected.

## ATTACHMENT II

### Fictitious Example – Aircraft Design and Manufacturer

The purpose of this attachment is to show a practical application of the system description process using a fictitious example of an aircraft design and manufacturing organization.

Throughout this narrative, certain details may be omitted to express the essence of the process, however, the reader should keep in mind that the process is necessarily an interactive, group exercise. Ideally the group will have core constituents and invite various members of the organization in to help expand the depth of the expertise at certain stages.

As the system identification process is executed, watch for hazard identification opportunities as the Procedural Document recommends. For any hazard noted in the system description, have a method to add it to the stack of hazards for later consideration. That is, while the process is described linearly, it is fine to jump ahead and move back throughout the process. In this presentation, whenever a discovered hazard is identified it will be noted as follows: **{HAZ: Defects in supply chain}.**

## Identify System

The company is looked at from three perspectives: organizational, processes and products. The assessment team decided the process and product domains would be analyzed together in this first step.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| The system identified is a multi-national aircraft design and manufacturing organization | {HAZ: Cultural and linguistic differences interpreting organizational information} |
| A multi-national company that has grown by acquiring other aircraft manufacturing companies | {HAZ: Conflicting procedures} |
| *Note:* The complete picture of the organization would have the subordinate organizations repeating the process described herein | |
| The design aspect includes support of retired designs from the legacies of the acquired companies, modification of designs for new variants and wholly new designs for emerging markets | |
| *Note:* The structure of the varying companies is represented by a high-level organization chart (high level organizational chart would be inserted here) | |
| The differing corporate entities often produce sub-assemblies of an aircraft in production | {HAZ: Defects introduced in moving sub-assemblies to final assembly} |
| The outcome of the company is to produce safe, reliable aircraft that generate a profit not only for the parent manufacturing company but also for the operator of the aircraft | |
| The parent company also seeks to successfully identify emerging markets for new aircraft designs | |
| Process and Product | |
| Parent and subordinate companies have developed a rich variety of proven methods to identify requirements, develop designs, conduct hazard analysis, supplier source selection, internal testing methods and approaches to certification conforming to various countries | |
| Methods have developed in accordance with standards such as AS9100, SAE standards, and 14 CFR Part 25 to name a few (cross references to these existing methods would be inserted here) | |

## Responsibilities, Authorities and Outcomes

The high-level organization chart used to identify the system is either re-used or expanded upon to show authority and responsibility within the company. The assessment team again decides to combine process and product domains in this step.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| Company consists of multiple, somewhat autonomous subsidiaries | {HAZ: Ill-defined authority across subsidiary boundaries} |
| The change management process of the parent company includes management of new acquisitions and identification of change in existing subsidiaries | |
| Process and Product | |
| Accountability is by product line, which is to say each aircraft has an accountable executive (AE) assigned | |
| The AE develops a team of leaders each responsible for varying facets of the aircraft be it in production or in operational support | {HAZ: Supervision, check/balance of AE} |
| For each aircraft, an organizational chart starting at the AE and descending through the team leaders is maintained and has a change management process | {HAZ: Loss of intellectual inventory when personnel retire or attrition} |

## Task Categories

Task categories are looked at from four areas: operational, administrative, supervisory, and resources. The product and process dimensions are combined in this example with focus only on the operational area across life cycle dimensions. Organizationally, the operational and supervisory perspectives were adequately described by the *Responsibilities, Authorities and Outcomes* step.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| The *administrative* dimension includes typical corporate functions such as human resources, marketing, accounting, etc. | |
| The *resource* dimension include items such as adequate lines of credit and cash reserves to operate the company, information technology systems, customer support systems and facilities management | {HAZ: Business continuity of information technology} |
| Process and Product | |
| The *requirements* life cycle contains methods for market analysis and iterative requirements identification methods leading to design specifications | {HAZ: Scope creep in requirements; requirements omissions} |
| The *design* life cycle includes CAD design techniques, wind tunnel analysis or simulations thereof, electronic simulations of human factors, creation of specifications for flight training simulators and type certification documentation | {HAZ: Incompatible software versions across supply chain} |
| When the aircraft is in *production*, task categories include management of logistics for sub-assembly integration, supply chain management, manufacturing automation setup and measurement of production rate and quality | {HAZ: Shortage of supply can stop assembly line}<br><br>{HAZ: Business continuity of shop floor automation logic (may differ from other information technology systems)} |
| The *delivery* life cycle includes certification of each aircraft produced, operational and maintenance manuals and end user training | {HAZ: Version management} |
| The *operations* life cycle requires task categories of product support and priority escalation of key issues, replacement parts, and participation by the company in use case analyses of aircraft operators (customers) to verify such use cases were considered during aircraft design, and participation in accident/incident investigation | {HAZ: Operator is planning on flying into gravel runway}<br><br>{HAZ: New hazards discovered may not feedback to full product lifecycle, i.e., requirements} |

| Item | Hazard (if identified) |
|---|---|
| When the company retires the product, methods exist to maintain adequate replacement parts for in-service aircraft | |

**System Analysis**

Using the SHEL – software, hardware, environment and liveware – heuristic, the system is analyzed along its organizational, process and product dimensions.

| | Item | Hazard (if identified) |
|---|---|---|
| Organizational | | |
| S | Employee job descriptions and goals as well as a company repository of policies and procedures maintained on the corporate intranet in addition to templates for engineering and safety processes | {HAZ: Version control across geographically disparate companies; different languages of employees (localization)} |
| H | The hardware perspective includes information technology support for a document management system, website and telecommunication capabilities, leases on facilities and equipment and maintenance of manufacturing tooling | {HAZ: Cyber attack}<br><br>{HAZ: Natural disaster; terrorism}<br><br>{HAZ: Obsolete tools} |
| E | Maintenance of a just culture and anonymous safety reporting programs, a safety council and legal agreements with suppliers and airframe organizations | |
| L | The liveware component contains the employee training for job functions and the promotion of the safety culture | {HAZ: New acquisitions may have inherent distrust of new parent} |
| Process | | |
| S | Electronic repositories of procedures to perform requirements, design, testing, production, quality measures, installation and field support | {HAZ: Intranet documents not available in all necessary areas due to security} |
| H | Production and office facilities along with shop tools and materials inventory | |
| E | Clean workplace, adequate ventilation, and safety control devices (i.e, hardhats, safety goggles, etc.) | |
| L | Adequate staffing of employees and proper training | |
| Product | | |
| S | Manuals for the end user, limitations and maintenance | {HAZ: Design features may make certain maintenance functions overly complex} |
| H | Raw materials supply as well as the need for simulators for aircrew training | |
| E | Atmospheric operating environments for the aircraft as well as the operator use cases for the aircraft in practice | {HAZ: Operator use cases may not match design} |
| L | How the product is used and maintained | {HAZ: Cabin configuration variants |

| | Item | Hazard (if identified) |
|---|---|---|
| | in operations as well as practical drift from designed operations and actual operations. Passenger comfort issues within the control of the manufacturer are also part of the system | impact on emergency egress} |

***Side Bar – Process Note***

*The reader should keep in mind throughout this process the end goal – the end goal is a hazard analysis. Each analysis point provides an opportunity to identify a hazard, as has been exemplified through the introduction of the* ***{HAZ: note}*** *notation. For example, if information technology fails to maintain the hardware for the website used to disseminate maintenance manuals, it is possible out of date documents could be published to customers and become one step in the path to an accident. The organization as whole makes up the safety management system, thus the importance of the analysis being conducted.*

## Work Dimensions

The next step in the system identification process is to look at work dimensions. One way to do so is to organize work dimensions as safety compatible and counter to safety (in the associated table, "✓" is for compatible, "✗" is for counter).

| | Item | Hazard (if identified) |
|---|---|---|
| | Organizational | |
| ✓ | Safety council and regulatory compliance objectives | {HAZ: Active engagement of safety council over time} |
| ✗ | Short-term profit and production goals | |
| ✗✓ | Organization of the company by subsidiary can be both safety compatible through specialization and expertise, but can also be safety counter if the subsidiaries fail to effectively communicate safety or productivity issues | |
| | Process | |
| ✓ | Quality measures used in the production processes and testing for certification | {HAZ: Wrong measures; unused measures}<br><br>{HAZ: Design to certification rather than to (higher) safety standard} |
| ✗ | Trying to avoid rework or use of disposable materials as well as overworking employees | |
| | Product | |
| ✓ | Minimum defects in delivery as well a rigorous certification process | |
| ✗ | Overuse of lightweight materials or low cost suppliers with insufficient controls on quality | |

## Decompose Activities

The work defined thus far has outlined a system. This step draws out specific activities that make up the broader system. This step can be a useful review of the prior steps and will often yield additions to prior steps in the process.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| Maintenance of the company organizational chart, annual benefits communication, supplier visits, industry conferences, employee performance reviews, monthly accounting and reporting, business continuity testing and information technology software and hardware upgrades | {HAZ: Non-competitive benefits may cause attrition of key personnel} |
| Process | |
| Requirement meetings, creation of CAD drawings, simulations, FMEA analysis, wind tunnel testing, tooling automation setup, time tracking, training and assembly of sub-assemblies | {HAZ: External component supplier may limit FMEA analysis depth} |
| Product | |
| Production of operator and maintenance manuals, advertising of new products, phone center activity to receive and process inbound communications, responses to critical safety concerns, accident investigation participation, and inventory counts | {HAZ: Escalation of safety issues may not be flagged} |

**Examine Interfaces**

Like decomposing activities, interfaces provide another retrospective opportunity.

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| The just culture may be taken advantage of by certain employee personality types | |
| Differing compensation between subsidiaries could cause intra-company transfers and associated retraining costs | |
| Information technology downtime effects nearly all processes of the company, regulatory violations can shut down production and supplier defects can compromise product integrity | {HAZ: Anti-virus software slows down computers; system maintenance causes down times at key production milestones} |
| Process and Product | |
| How the aircraft operators choose to operate the aircraft – operational use cases may not be those anticipated in design (as mentioned earlier) | |
| Operating manuals and specifications may not match the current revision of the production aircraft | |
| Design and production changes require updates to hazard/risk analysis | {HAZ: Workflow for production changes may be incomplete} |
| Defects discovered in operations may require corrective actions such as airworthiness directives | |

**Environmental Impacts**

| Item | Hazard (if identified) |
|---|---|
| Organizational | |
| Intellectual sabotage, patent infringement, natural disasters destroying production facilities, information technology systems failures, employee turnover, economic downturns, accidents in production or in operations, and regulatory changes to airworthiness requirements | {HAZ: Lack of involvement in regulatory change process in differing jurisdictions} |
| Process | |
| Changes to requirements, tooling failures in production, obsolescence of necessary tooling, and practical drift in production processes | |
| Product | |
| Actual environments differing from the design environment, undetected product flaws entering the operational environment, component incompatibilities | {HAZ: Component failures may be reported to component manufacturer, not to aircraft manufacturer} |
| Simulator behaviors do not match the actual characteristics of the aircraft | {HAZ: Simulator trained techniques may not match anticipated design} |

## Hazard Identification

The system analysis should have spawned numerous opportunities to identify hazards in the system, again broken down by organization, process and product. Within this example, the process produced many hazards, but still only a subset of what an actual execution of the process would yield. The list that follows is only a small fraction of the total hazards that could be identified from the system analysis. Furthermore, it includes a summary of the hazard items identified as well as new hazards this step itself introduces.

| Organizational |
|---|
| Out of date organizational chart and poor definition of authority and responsibility |
| Information technology security breach |
| Accidents lead to product liability claims |
| Wrong product developed – no market |
| Polices and procedures do not keep up with best practices |
| Failure of just culture to penetrate throughout company |
| Regulations in different countries impact productivity |
| Process |
| Sub-assembly integration logistical failures |
| Remote located CAD systems may not use the same software version causing incompatibilities |
| Poor training on production processes |
| Poor measurement of production metrics |
| Product |
| Component/sub-assembly failure in operations |
| Simulator behavior does not match aircraft behavior |
| Maintenance errors |
| Operator errors including practical drift |
| Unexpected environmental factors |
| Unexpected operator use cases |

## Conclusion

The system description of the company as well as hazard identification is the foundation of a safety management system. It should become clear by the time the analysis is executed that the system analysis herein is a *macro* view of the company. What follows the macro view are numerous *micro* views of many supporting processes: a similar analysis and hazard identification procedure can and should be executed for each process within the company.

Of course for each hazard the associated risks must be drawn out and an assessment made of the likelihood and severity of such risks. For those risks deemed unacceptable, controls must be put in place and then assurance processes put in place to verify the controls behave as expected.