Paper
Int'l J. of Aeronautical & Space Sci. 16(3), 451–462 (2015)
DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451

IJASS
International Journal of Aeronautical and Space Sciences

Roles of Safety Management System (SMS) in Aircraft Development

Won Kwan Lee* and Seung Jo Kim**

Department of Aerospace Engineering, College of Engineering, Seoul National University, Seoul 08826, Korea

Abstract

Safety is the first priority in civil aviation, and so the International Civil Aviation Organization (ICAO) has introduced and mandated the use of Safety Management Systems (SMS) by airlines, airports, air traffic services, aircraft maintenance organizations, and training organizations. The aircraft manufacturing industry is the last for which ICAO has mandated the implementation of SMS. Since SMS is a somewhat newer approach for most manufacturers in the aviation industry, they hardly believe in the value of implementing SMS. The management of safety risk characteristics that occur during early aircraft development stages and the systematic linkage that the safety risk has to do with an aircraft in service could have a significant influence on the safe operation and life cycle of the aircraft. This paper conducts a case analysis of the McDonnell Douglas MD-11 accident/incident to identify the root causes and safety risk levels, and also verified why aircraft manufacturing industry should begin to adopt SMS in order to prevent aircraft accident.

Key words: Safety Management System (SMS), Aircraft Manufacturing Industry, Design and Certification Processes, Human Factor Classification Analysis System (HFACS), Accident Prevention

1. Introduction

In the aviation industry, complex and advanced systems are constantly being developed and introduced. Although the reliability of aircraft has systematically improved as the advanced technology is further developed, the organizational and human factors that interact with those systems are the fundamental causes of the accidents [1, 2]. Due to the demand for a more efficient approach to manage safety in order to cope with these changes, Safety Management Systems (SMS) is currently being viewed as effective, systemic management models.

Quality Management System (QMS) is well known throughout the industry, and is also included in ICAO Annex 8 (Production Authorization) and Annex 6 Part I (Maintenance Organization). It is also settled in the aircraft manufacturing industry. In contrast, SMS was established somewhat later than QMS, and was systematically reflected on ICAO annexes for airlines, air traffic control, airports, maintenance organizations, and training organizations. The aircraft manufacturing industry is the last group for which ICAO has mandated the implementation of SMS.

Since SMS is a somewhat newer approach for most manufacturers in the aviation industry, they hardly recognize the value of implementation of SMS. Compared to SMS, Stolzer verified that QMS does not specifically cover risk management and controls [3]. QMS and SMS are similar in many ways, but there is a big difference. SMS is focused on safety, human and organization, and satisfaction of safety, whereas QMS is focused on product, service, and customer satisfaction [4, 5].

SMS is intended to concentrically monitor safety performance, identify safety hazards, evaluate related risks, and manage the risks effectively. In contrast, QMS is concentrated on compliance with regulations and requirements in order to satisfy customer expectations and requirements on the contracts. QMS is focused on products and services with certain level of quality consistency satisfying customer expectations and requirements.

QMS has independent Quality Assurance which allows

* Ph. D Candidate, Qualified International Air Transportation Association (IATA) Operational Safety Lead Auditor, and General Manager- Corporate Safety, Quality, and Compliance Audit, Korean Airlines
** Professor, Corresponding author: sjkim@snu.ac.kr

Received: May 13, 2015 Revised: June 25, 2015 Accepted: July 11, 2015

http://ijass.org pISSN: 2093-274x eISSN: 2093-2480

utilization of feedback connection process, in order to guarantee supply of products and services, with no defects and appropriate for its purposes. On the other hand, Safety Assurance focuses on ensuring risk controls which meets safety objectives. Please refer to the relevant safety and quality definitions in Table 1 [4, 5].

Safety can be defined as freedom from those conditions that can lead to death, injury, occupational illness, and damage to or loss of equipment or property under stated conditions. Freedom from all hazardous conditions, which means absolute safety, is nearly impossible to achieve. Therefore, safety can be practically defined as maintaining an acceptable level of risk in order to prevent accidents. [4, 5].

Reliability can be defined as the ability of the system to maintain its required functions under stated conditions for a specified period of time. Failure is the system, subsystem, component or part's inability to fulfill the required functions under specified conditions for a specified duration.

In addition to QMS, aircraft manufacturing industry is required to perform aircraft Functional Hazard Analysis as a part of the type certification process. The Functional Hazard Analysis is conducted to identify failure condition and improve failure rates. Failure of critical subsystem or component may result in unsafe conditions and/or acts. For example, a manufacturer has underestimated failure rate of the lithium-ion batteries on B787 aircrafts. The manufacturers assessed that the rate of occurrence of fire and/smoke due to lithium-ion battery failure would be about one in 10 million flight hours. However, that prediction for failure rate was significantly lower than the actual failure rate [6]. B787's battery's failure was first observed at 52,000 hours of service. The fleet had been grounded for more than 3 months until redesign of lithium-ion battery was completed for safety purposes. This kind of unsafe condition could be prevented by more effective use of Functional Hazard Analysis methodologies. Under these circumstances, such improvement can reduce the possibility of accidents caused by component failures.

System safety is the application of engineering and management principles, criteria, and techniques to achieve an acceptable level of safety throughout all phases of a system. Achieving this definition of system safety is the primary objective of SMS [3]. It might be unsafe when the elements of system safety are not considered enough in the reliability of product design. For example, a windproof lighter may be highly reliable and safe when it is used under the normal

Table 1. Safety and Quality relevant Definitions [4, 5].

SMS (Safety Management System)	QMS (Quality Management System)
• SMS is focused on safety performance. The objectives of an SMS are to identify safety related hazards, assess the associated risk, and implement effective risk controls. • SMS is to identify safety related hazards the organization must confront, and to control the associated risks. SMS is designed to manage safety risk and measure safety performance during delivery of products and services. The safety risk management process eliminates hazards or provides effective controls to mitigate safety risks by maintaining an appropriate resource allocation balance between production and protection to meet safety performance requirements.	• QMS is focused on compliance to prescriptive regulations and requirements, to meet customer expectations and contractual obligations. • QMS focuses on the consistent deliver of products and services that meet relevant specifications • A QMS provides consistency in the delivery of products and services to meet performance standards as well as customer expectations. The QMS also has an independent assurance function that utilizes a feedback loop to assure delivery of products and services that are ―fit for purpose and free of defects or errors.
• A systematic approach to managing safety within an organization, including the necessary organizational structures, accountabilities, policies and procedures. As a minimum, an SMS: – Identifies safety hazards; – Ensures that remedial action necessary to maintain an acceptable level of safety is implemented; – Provides for continuous monitoring and regular assessment of the safety level achieved; and – Aims to make continuous improvement to the overall level of safety.	• The aggregate of the organizational activities, plans, policies, procedures, processes, resources, responsibilities, and the infrastructure implemented to ensure all operational activities satisfy the customer's and the regulatory requirement. A controlled documentation system is used to reflect the plans, policies, procedures, processes, resources, responsibilities and the infrastructure used to achieve a continuous and consistent implementation and compliance.

DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451

conditions. However, when it is used close to flammable paint or a gas station, it is still very reliable but unsafe. Safety is always a primary concern, and the designers do everything possible to mitigate known problems. However, designers face with many different aspects besides safety, such as fuel efficiency and passenger comfort. Most systems currently have some ways of preventing unsafe acts such as redundant systems and safety procedures. However, no system is completely safe, and unsafe acts do occur. The area involving safety issue has broader meaning than the reliability. For prospective system safety, it is necessary to consider not only component failure but also system design, actual operating environments, human factor, and organizational factors.

Kinnersley and Roelen [7] have validated approximately 50-60% of root cause of accidents were in design stage. In addition, their study mentioned that investigations do not always allow classification of the failure according to the design stage [7]. These investigations were conducted with the aim for preventing similar accidents. Also, practical short-term solutions to identified problems are usually operational, training, etc. So the importance of design is not always highlighted in the investigation [7].

Most of the aircraft manufacturer already has established QMS and reliability program. Identification of hazards associated with organizational factors, including human performance within an organization is a paradigm shift to systemic safety management. By understanding systematic safety problems but not problems within the individuals which lead accidents to occur, the first step towards SMS is taken as effective systemic management solution to prevent accidents.

Therefore, this paper is focused on analyzing a case study of the severe hard/bounced and tail strike landings of McDonnell Douglas MD-11 aircrafts to identify the root causes and safety risk levels. This paper has also verified why aircraft manufacturing industry should begin to adopt SMS in order to manage safety risks with a systemic safety management approach in order to prevent aircraft accidents.

2. Safety Management

2.1 SMS legislation background

SMS is a top-down organization-level approach to managing risk and safety. This process consists of an analysis of safety data and risk mitigation in order to minimize accidents and incidents [4, 5].

The International Civil Aviation Organization (ICAO) published the Safety Management Manual (Doc 9859) in 2006 to better understand SMS, and the 3rd edition was published in 2013. ICAO defines a safety management as a system-level process to manage safety, including in areas of organization systems, reasonability, policies, and process [4, 5]. As can be seen in Table 2 [8], beginning of 2001, SMS requirements have been expanded across the entire aviation industry, including airlines, aircraft maintenance organizations and training organizations, starting from the ICAO annex 11 (Air Traffic Service) and 14 (Aerodromes). Recently the ICAO annex 8 was revised and SMS requirements were expanded to the aircraft manufacturing industry. In addition, the new Annex 19 (Safety Management) was established as of July 2013,

Table 2. ICAO Annex and SMS requirement [8].

Safety Management SARPs for Service Providers			
Annex	Intended Audience	Denomination	Date Applicable
11	Air traffic services providers	Safety Management Programme	Nov, 2001
14	Certified Aerodromes	Safety Management Programme	Nov, 2001
2005 – Harmonization of Safety Management SARPs			
6, 11 and 14	A/C Operators & AMOs	SMS	Jan, 2009
2008 – 2nd Harmonization of Safety Management SARPs			
1	Training Organizations	SMS	Nov, 2010
8	Manufacturers	SMS	Nov, 2013
1, 6, 11, 14		SMS Framework	Nov, 2010

which was the first in 30 years and the annex includes basic guidelines for safety management. In order to comply with the ICAO SMS Standards, the aviation authorities of each member nations must establish a State Safety Program (SSP), which is a basic program that manages safety and risk by setting up integrated nationwide safety objectives and safety indexes. Under SMS rules, the aviation industry is required to adopt and implement SMS as well.

Failure to meet ICAO SMS standards will impair the ability to operate internationally [9], and ensuring compliance with the ICAO SMS standards could be a strong source of competitiveness in the global aircraft market. The Federal Aviation Administration (FAA) has plans to adopt SMS in the Bilateral Aviation Safety Agreement (BASA) program after completion of SMS rulemaking in FAA Part 21 [10]. When a new country signs the BASA agreement with U.S.A, it is expected that their aircraft and/or products can be exported in the global market. Therefore, doing so will be required preparing and establishing SMS in order to fulfill the ICAO and FAA requirements.

2.2 SMS Components

SMS consists of 4 major components, and 12 elements as shown in Table 3 [4, 5]. The key elements of the SMS concept which are new to certification process are Safety Risk Management and Safety Assurance.

2.3 Safety Risk

Hazards are defined as existing or potential causes or factors that can result in the loss of human lives, system, equipment, properties, etc. [4, 5]. Risk is described as the level of the risk that is measured according to the severity and probability of the potential for hazard. The type of risk mentioned in this paper is constrained to safety risks involved in the operation of aircraft, and not financial or economic risks. Risk management intends to measure, recognize, and analyze risk factors that can disrupt and threaten the operation of the organization. Risk management is described in terms of maintaining an acceptable level of the risk as well as to eliminate and/or reduce such risk. Thus risk management allows for top management to make decisions that balance the allocation of resources according to the safety data and analysis [11].

Safety Risk Management (SRM) and Safety Assurance (SA) are key SMS functions that are part of the decision-making process outlined Fig. 1 [12]. Fig. 1 shows how the

Table 3. SMS Components [4, 5].

(1) Safety Policy and Objectives
The commitments of the top management level to determine methods, procedures, organizational structure for achieving constant improvement on safety and safety goals.

Element 1: Management commitment and responsibility (Safety Policy)
Element 2: Safety accountabilities
Element 3: Appointment of key safety personnel
Element 4: Coordination of emergency response planning
Element 5: SMS documentation

(2) Safety Risk Management
Determination of the appropriateness and necessity of new or updated risk management based on safety decision-making and acceptable level of the risk.

Element 6: Hazard Identification
Element 7: Safety risk assessment and mitigation

(3) Safety Assurance
Evaluate the continued effectiveness of implemented risk control strategies and support on identifying new hazards.

Element 8: Safety performance monitoring and measurement
Element 9: The management of change
Element 10: Continuous improvement of the SMS

(4) Safety Promotion
Education/training, communications, and other activities for safety promotion which makes the positive safety culture in all areas of the organization.

Element 11: Training and education
Element 12: Safety communication

DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451

SRM and the SA functions are related to one another. SRM is a process that can be used to initially identify hazards and to assess risk. This risk analysis process includes an analysis of potential consequences of operation with the identified presence of the hazards. Risk Controls have been developed to mitigate risk to an acceptable level, and it is thus determined to be acceptable to operate within these hazards.

After a system has been designed or redesigned using the SRM process, the new or revised system should be closely monitored with the continuous use of the SA process. The SA interacts with SRM to ensure that risk controls are practically in effect and that they continue to obtain their intended level of acceptable risk through continuous measurement and monitoring of the performance of the system.

As in SRM, safety data must be analyzed to engage in risk-based decision making. In the case of SA, several paths can be taken as a result of the decision-making process. If the data and analysis indicate that the system and its risk controls function are at the intended risk level, the results are satisfactory and management can now ensure the safe operation of the system. One of the most important functions of the SMS is to predict the vulnerable area where risk management is required through systematic analysis of safety information. SMS' function also includes ensuring safety through extensive proactive management under the effective SRM and SA. In the case where the risk controls have not achieved their intended objective, action should be taken to correct the problem. In the case where the system is being used as intended and the expected results are not produced, the design of the system should be reconsidered by tracing the path back to the SRM process [12] since doing so is an especially important role of the SA process.

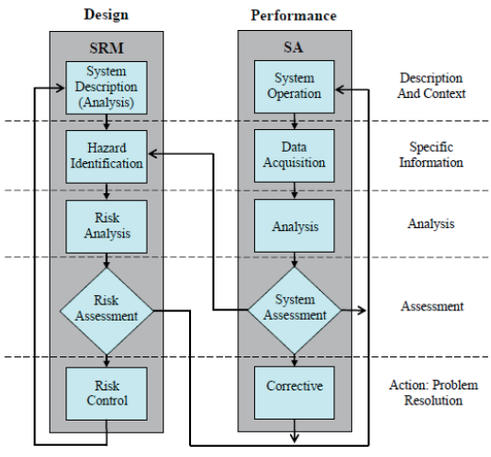

Fig. 1. Safety Management Decision making Process [12].

3. Analysis

As can be seen Table 4, a total of 19 MD-11 severe hard/bounced and tail strike landings accidents/incidents were occurred between 1993 and 2013[13]. In this analysis, two analysis models can be used to identify the root causes and safety risks level with their investigation reports. The Human Factors Analysis and Classification System (HFACS) can be used for the root causal analysis, and the FAA Transport Airplane Risk Assessment Methodology (TARAM) can be used for risk assessment.

3.1 Accidents/incidents review

MD-11's center of gravity was designed to be located much further aft compared to other commercial aircraft to improve fuel efficiency. However, this has resulted in sensitivity in the control column. This type of design, which is referred to as "Relaxed Stability", is commonly applied to fighter jets and is the first attempt to commercial aircraft. This could result in excessive control during recovery due to the oscillation of aircraft during bouncing or a hard landing and can also serve as a factor that makes the situation more serious.

A total of 19 MD-11 have experienced severe hard/bounced and tail strike landings since first time that the fleet was entered into service in 1990. The National Transportation Safety Board (NTSB) has determined that the MD-11's controls were more sensitive than those of other airplanes, especially at low speed and altitude [14]. In order to compensate for the smaller empennage, the Longitudinal Stability Augmentation System (LSAS) continuously trims the stabilizer under computerized controls [15].

In contrast to other commercial aircrafts, the MD-11 requires a unique landing technique to compensate for its tendency to pitch up. This requires for the pilot to first push the control yoke as soon as the aircraft touches down and extend the spoilers. Then the pilot is to pull the control yoke as soon as the auto brake is applied in order to softly lower the nose of the aircraft. In most of the cases, the unexpected hard touchdown had made other pilots to overcompensate the controls, resulting in tail strike. Pilots, who are aware of this, are also trained to know that a tail strike can easily follow a hard landing. They are also particularly aware of any pitch up on landing. Repeated botched landings can result in a hazardous bounce, wing fractures and sometimes even rolling on the runway, such as FedEx accidents occurred in Newark and Narita. Other examples include China Airlines accident occurred in Hong Kong, and Lufthansa Cargo accident occurred in Saudi Arabia.

3.2 Causal Factor Analysis using the HFACS Model

3.2.1 Overview of HFACS

As can be seen in Table 5 [16-17], HFACS was developed by Dr. Scott Shappell and Dr. Douglas Wiegmann based on Dr. James Reason's "Swiss Cheese" model, and it is used as a tool for causal factor classification and root causal analysis. The purpose of this tool is to break up a potential accident/incident chain by expanding the Unsafe Acts to Organizational Factor and to manage hazards more systemically.

The Australian Transport Safety Bureau analyzed 2,025 accident reports from 1993 to 2003 of airlines in their jurisdiction by using HFACS. The results of the analysis indicated that HFACS can be considered as a predictive tool for SMS. Fig. 2 shows the relationships between Unsafe Acts and higher levels of HFACS. This indicates that an analysis of the Unsafe Supervision of HFACS could predict the "Precondition for Unsafe Acts", as well as "Unsafe Acts" that cause accidents [18].

Recently, even International Air Transportation

Table 4. List of accidents/incidents [13].

McDonnell Douglas MD-11 Severe Hard/Bounced and Tail strike Landings			
	Date	**Location**	**Operator**
1	30 APR 1993	Los Angeles	Delta Airlines
2	19 AUG 1994	Chicago	Alitalia
3	21 JUN 1997	Honolulu	Garuda
4	31 JUL 1997	Newark	FedEx
5	22 AUG 1999	Hong Kong	China Airline
6	22 MAY 2000	Taipei	Eva Air
7	20 NOV 2001	Taipei	Eva Air
8	7 JUN 2005	Louisville, Kentucky	UPS
9	23 MAR 2009	Tokyo	FedEx
10	3 JUN 2009	Urumqi	China Cargo
11	9 JUN 2009	Khartoum	Saudi Arabian
12	13 SEP 2009	Mexico City	Lufthansa Cargo
13	20 OCT 2009	Montevideo, Uruguay	Centurion Air Cargo
14	28 NOV 2009	Shanghai	Avient Aviation
15	27 JUL 2010	Riyadh, Saudi Arabia	Lufthansa Cargo
16	22 SEP 2010	Kabul, Afghanistan	World Airways
17	13 OCT 2012	Sao Paolo, Brazil	Centurion Air Cargo
18	25 JAN 2013	Denver	FedEx
19	24 NOV 2013	Sao Paolo, Brazil	Lufthansa Cargo

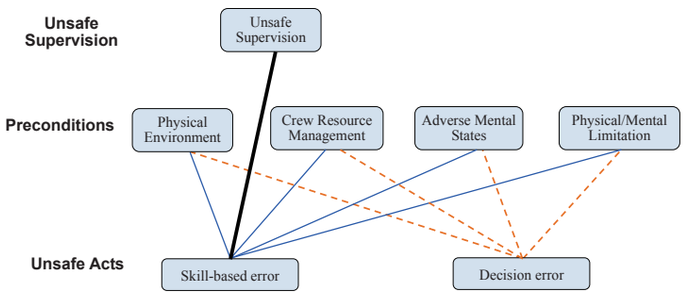

Fig. 2. Relationships between Unsafe Acts and higher levels of HFACS [17].

DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451

Association (IATA) introduced the HFACS concept across all Global Audit Programs and has started using the HFCAS model as a fundamental categorization and causal factor analysis tool for Audit Findings. HFACS's High-level causes can be identified and analyzed to predict Unsafe Acts before an accident or incident occurs. In addition, HFACS can be considered to be a predictive tool for SMS. Table 5 [16-17] shows a brief description of the causal HFACS categories.

3.2.2 Results

We have evaluated 19 cases of severe hard/bounced and tail strike landings of MD-11 aircrafts in this study. From these 19 accident/incidents, a total of 101 causal factors were identified and used for analysis. As can be seen on Table 6, causal factors are involved throughout 4 HFACS levels. Within the category of Unsafe Acts of Operators, the most frequently cited form of error was Decision Errors. With regard to the Preconditions for Unsafe Acts, the majority of causal factors have involved the Physical Environment and Technical Environment. In the level of Unsafe Supervision, Inadequate Supervision and Failed to correct known Problem were identified. Typically, fewer causal factors were identified at the Organizational Influence levels. However, at this time, the number of the Organizational Process and

Table 5. Description of HFACS causal categories [16-17].

ORGANIZATIONAL INFLUENCES
Organizational Climate (OC): Prevailing atmosphere/vision within the organization including such things as policies, command structure, and culture.
Operational Process (OP): Formal process by which the vision of an organization is carried out including operations, procedures, and oversight among others.
Resource Management (OM): This category describes how human, monetary, and equipment resources necessary to carry out the vision are managed.
UNSAFE SUPERVISION
Inadequate Supervision (SI): Oversight and management of personnel and resources including training, professional guidance, and operational leadership among other aspects.
Planned Inappropriate Operations (SP): Management and assignment of work including aspects of risk management, crew pairing, operational tempo, etc.
Failed to Correct Known Problems (SF): Those instances when deficiencies among individuals, equipment, training, or other related safety areas are "known" to the supervisor, yet are allowed to continue uncorrected.
Supervisory Violations (SV): The willful disregard for existing rules, regulations, instructions, or standard operating procedures by management during the course of their duties.
PRECONDITIONS FOR UNSAFE ACTS
Environmental Factors
Technological Environment (PET): This category encompasses a variety of issues including the design of equipment and controls, display/interface characteristics, checklist layouts, task factors and automation.
Physical Environment (PEP): The category includes both the operational setting (e.g., weather, altitude, terrain) and the ambient environment, such as heat, vibration, lighting, toxins, etc.
Condition of the Operator
Adverse Mental States (PCM): Acute psychological and/or mental conditions that negatively affect performance such as mental fatigue, pernicious attitudes, and misplaced motivation.
Adverse Physiological States (PCP): Acute medical and/or physiological conditions that preclude safe operations such as illness, intoxication, and the myriad of pharmacological and medical abnormalities known to affect performance.
Physical/Mental Limitations (PCL): Permanent physical/mental disabilities that may adversely impact performance such as poor vision, lack of physical strength, mental aptitude, general knowledge, and a variety of other chronic mental illnesses.
Personnel Factors
Communication, Coordination, & Planning (PPC): Includes a variety of communication, coordination, and teamwork issues that impact performance.
Fitness for Duty (PPR): Off-duty activities required to perform optimally on the job such as adhering to crew rest requirements, alcohol restrictions, and other off-duty mandates.
UNSAFE ACTS
Errors
Decision Errors (AED): These "thinking" errors represent conscious, goal-intended behavior that proceeds as designed, yet the plan proves inadequate or inappropriate for the situation. These errors typically manifest as poorly executed procedures, improper choices, or simply the misinterpretation and/or misuse of relevant information.
Skill-based Errors (AES): Highly practiced behavior that occurs with little or no conscious thought. These "doing" errors frequently appear as breakdown in visual scan patterns, inadvertent activation/deactivation of switches, forgotten intentions, and omitted items in checklists often appear. Even the manner or technique with which one performs a task is included.
Perceptual Errors (AEP): These errors arise when sensory input is degraded as is often the case when flying at night, in poor weather, or in otherwise visually impoverished environments. Faced with acting on imperfect or incomplete information, aircrew run the risk of misjudging distances, altitude, and decent rates, as well as responding incorrectly to a variety of visual/vestibular illusions.
Violations **(V)**
Routine Violations (AVR): Often referred to as "bending the rules" this type of violation tends to be habitual by nature and is often enabled by a system of supervision and management that tolerates such departures from the rules.
Exceptional Violations (AVE): Isolated departures from authority, neither typical of the individual nor condoned by management.

Oversight identified is similar to the number of Unsafe Supervision and Preconditions for Unsafe Acts. It means organizational levels of corrective actions are needed in order to fundamentally improve.

As can be seen in Fig. 3, there were no significant changes on Decision Errors from 1993 to 2013. The lines were essentially flat on the graph, showing that any interventions aimed at reducing specific types of human error prior to, or during this time period did not appear to have any long term influences. Despite the attempts, errors still do exist today.

Decision Error is the most common type of error associated with aircraft operations. It assumes that each individual has the knowledge of the procedure. However, an operator may perform a task incorrectly simply because they do not know the correct procedure either due to lack of training or the inability to retain information. Regardless, these types of errors suggest that specific training or new cockpit system aids, and cues are necessary to assist MD-11 pilots to make better decision and improve pilot reactions.

24 factors were observed in the level of Precondition of Unsafe Acts (Physical/Mental Limitation, Communication and Coordination, Physical Environment, Technological Environment). Among these, Technological Environment was the most frequently identified precondition. MD-11's

Table 6. MD-11 Frequency of cases associated with causal code categories.

HFACS category	**n**
Organizational Influence	**20**
Resource Management	
Budget Resource	1
Organizational Process	
Procedure	8
Oversight	11
Unsafe Supervision	**21**
Inadequate Supervision	
Inadequate Supervision of Training	10
Inadequate Supervision of Guidance/ Oversight	1
Failed to correct known Problem	
Failed to correct known risky problems	10
Preconditions for Unsafe Acts	**24**
Condition of Operator	
Physical/Mental Limitation	4
Personnel Factors	
Communication and Coordination	3
Environmental Factors	
Physical Environment	2
Technological Environment	15
Unsafe Acts	**36**
Decision Error	35
Skill-Based Error	1

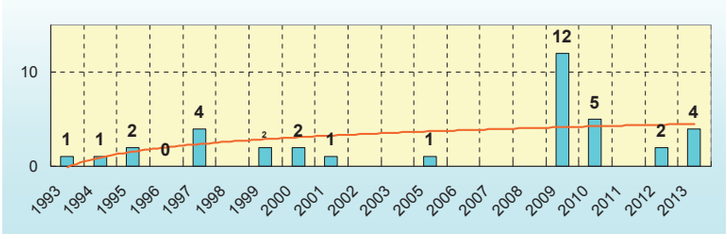

Fig. 3. Decision Errors from 1993 to 2013.

DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451

characteristics include light control force and its tendency to have a nose up landing. It was expected that this unique design have influenced multiple severe hard/bounced and tail strike landings.

21 factors of unsafe supervision were identified in the analyzed cases. The majority of causal factors at this level fell into the "Failed to correct known risky problems" and "Inadequate design of training program."

20 factors of organizational influence were identified and 19 of those fell into the "Inadequate training/procedures/guidance" and "Inadequate training oversight." Three years after the Newark accident which had occurred in 1997, FAA has issued Advisory Circular 120-71, "Standard Operating Procedures for Flight Deck Crew Members" and Bulletins to discuss stabilized approaches and reduction of accidents during approach and landing. However, these were generic guidelines, and not sufficient or effective for MD-11's particular safety problems.

3.3 Risk Assessment used by the FAA TARAM

3.3.1 Overview of TARAM

TARAM was developed for FAA aerospace safety engineers to calculate the specific levels of risk associated with identifiable design flaws in transport airplanes. Detailed instructions and guidance are given in terms of using the risk analysis calculations when making safety decisions. According to TARAM [19], risk associated with a single continued operational safety issue should not result in individual risk above 10^{-7}/hr. The level of individual risk may require urgent action, and it was concluded that urgent action is required halfway between the 10^{-5}/hr and 10^{-7}/hr safety level [19].

The following are the risk assessment equations that are described in the FAA TARAM handbook [19].

$$\text{Fleet exposure: } U \times T \times \Sigma \quad (1)$$

$$\text{Predicted number of Occurrences: } U \times T \times \Sigma \times F \quad (2)$$

where U is the utilization, the average flight hours, T is the time, and Σ is the Number of Airplanes.

$$\text{Severity: } S = IR \quad (3)$$

where IR is the injury ratio that indicates the average single-event probability that those exposed to a particularly dangerous event will suffer a fatal injury.

$$\text{Fleet Risk: } R = (U \times T \times \Sigma \times F) \times CP \times S \quad (4)$$

$$\text{Individual risk: } R = F \times CP \times S \quad (5)$$

where CP is the probability that the particular condition under study will result in a dangerous event with a known severity.

The frequency of the occurrence (F) is defined as the expected rate at which the condition that is under study will occur within the affected fleet. These can be calculated as the number of occurrences divided by total fleet flight hours.

3.3.2 Results

"Individual Risk" is defined as the probability of a fatal injury per flight hour, and the "Fleet Risk" is defined as a constant failure rate in the FAA TARAM handbook [19]. According to TARAM, cases where sufficient practical data is not available involve the accepted engineering practices of determining the "best estimate" of the actual quantitative values needed to determine risk.

The calculation of F for the individual risk and fleet risk for MD-11 severe hard/bounced and tail strike landings is as follows.

$F = 19/2{,}490{,}000 \text{ hrs.} \cong 7.6 \times 10^{-6}$/hr.

where 2,490,000 represent total fleet flight hours and 19 occurrences took place for the MD-11 severe hard/bounced and tail strike landings.

CP = 0.333

IR= 0.5

Individual Risk = $(6 \times 10^{-6}/\text{hr.}) \times 0.333 \times 0.5$

, where 0.333 (CP) and 0.5 (IR) was estimated.

Individual Risk $\cong$ $\mathbf{4 \times 10^{-7}}$/hr.

Fleet Risk = $(1{,}300{,}000^* \times 6 \times 10^{-6}/\text{hr.}) \times 0.333 \times 0.5 \cong$ **1.3**

*To determine the fleet exposure, instead of using Equation (1), the estimated flight hours were compared to the actual fleet flight hours of aircraft of a similar size and with the operating time periods.

The TARAM guideline for normally accepted individual risk values is below 1×10^{-7}/hr. The actual outcome of the individual risk values was 4×10^{-7}/hr for MD-11 and it was above an acceptable level. The TARAM guidelines for the normally accepted fleet risk are below 0.02. The actual levels from MD-11 were 1.3, which is greater.

4. Discussion

4.1 MD-11 Safety Records

200 MD-11s have been manufactured over the last ten years since the first delivery on November 1990. In the case of the A330, which was first delivered in 1993 during a similar time period as the MD-11, the accumulated number of orders is 1174 as of March 2015. The production of MD-11 came to a halt in 2000 due to the failure to receive further orders. Since it was no longer desired for the passenger plane market, many

air carriers converted their MD-11s to cargo aircrafts.

The MD-11 suffered 19 severe hard/bounced and tail strike landings accidents between 1993 and 2013, which is the highest rate of such dangerous touchdowns based on the number of flights among Western-built jet models. Normally, each new generation of airliner crashes less frequently than past models. In terms of aircraft losses per million departures, the MD-11 has been lost 10 times more than the Boeing 747-400, which was introduced in 1989 with similar technology. The MD-11 has also been lost 15 times more than older 757 and 767 models [20].

4.2 Safety Risk Management

HFACS is one of the useful SMS tools to identify and mitigate the true causes of hazards, incidents and accidents. We have verified that the root causes of MD-11 accidents/ incidents could be classified into HFACS's higher level, which refer to the management of the design and certification process. According to research in Austria [18] , accidents/ incidents could be predicted and prevented if HFACS's higher level, such as Unsafe Supervision and Organizational Influence, were closely monitored, identified, and effectively managed.

Through an analysis using the FAA TARAM model, we have examined that the risk level of the severe hard/ bounced and tail strike landings of MD-11 aircrafts is still at the unacceptable level. This indicated exactly how important it is to manage safety risk from the beginning of the aircraft design process, and to systematically link this safety risk after the aircraft is entered into service, since this can have a significant influence on the safe operation and life cycle of the aircraft. QMS and reliability program were not enough for managing safety risk throughout aircraft life cycle. SMS is an effective tool to identify, assess, and mitigate safety risks more systemically, by using proactive and predictive methods of safety risk management rather than reactive.

It is difficult to understand that certain organizational decisions could impact the safety of a product. Even though FAA's corrective actions in 2000, MD-11 crews continue to have difficulty in judging the appropriate operations to avoid or recover from the hard landings, and 13 more accident/ incidents were occurred after that. It's because the FAA's generic guidance for MD-11's particular safety problem was not sufficient or effective. Through the analysis of Decision Errors by HFACS, it was verified that any interventions aimed at reducing unsafe acts prior to, or during this time period did not appear to have any long term impact. The MD-11 aircrafts are still suffering severe hard/bounced and tail strike landings to date. After the system has been designed or redesigned using the risk assessment process, the new or revised system, procedure, or any other should be closely monitored by continuously using the SA process. The SA interacts with SRM to ensure that risk controls are practically in effect and that they continue to obtain their intended level of acceptable risk through continuous measurement and monitoring of the system performance. With effective SRM and SA, potential risk of MD-11 aircrafts' severe hard/bounced and tail strike landings could be managed and prevented.

The landing environment brings many challenges for the pilot. Pilots make control inputs based on their perceptions and experiences. When approaching for landing, the pilot must align the aircraft with the runway, and then manage the descent rate to perform a smooth touchdown. This also must occur within the appropriate touchdown zone, which will enable the aircraft to safely stop with enough runway remaining. Once main landing gears make contact to the ground, the pilot will lower the nose of the aircraft to the ground, and apply reverse thrust and brakes to stop the aircraft. This is extremely dynamic environment, which requires a repetitive cycle of perception, action, and feedback from the environment with immediate corrections to any unexpected situations. Pilots, like all other human, cannot be expected to deal with a problem they do not know about beforehand. Pilot maybe placed into a position where their perceptions do not match the actual aircraft dynamics and operational environments. According to HFACS's analysis, Technological Environment was the most frequently identified precondition for MD-11's Unsafe Acts. MD-11's characteristics of the new design were added on extremely dynamic landing environment, and significantly influenced pilot's unsafe acts. The area involving safety problem has broad meaning than that of reliability problem. For system safety prospective, under the unexpected conditions, more complicated outcomes were occurred based on organizational and human factor that interacts with those systems. It was required to consider not only reliability of component but also system design, dynamic operational environment, human factor, and organizational factors. MD-11's potential risk for severe hard/bounced and tail strike landings could be controlled and/or mitigated if it was systemically handled based on these factors; aircraft's landing characteristics, actual landing environment, pilot's perception and reactions in the organizational and human factors prospective.

5. Conclusion

In cases where aircraft accidents and incidents are exposed to public, the cost is tremendously high. As we have

seen through the case study of MD-11, successful aircraft development in the global market depends on identifying safety risks and mitigating these risks through systematic management of safety. By adopting and implementing SMS required by ICAO in aircraft manufacturing industry will improve managing safety risk and operational safety. SMS is a very effective solution to safety risk management for the currently complex aviation industry that is continuously introducing new technologies [9, 21-22].

Most of the aircraft manufacturing industries already had QMS and reliability program as part of their aircraft certification process. Identification of hazards associated with organizational factors, including human performance within an organization, is a paradigm shift to systemic safety management. SMS is intended to identify safety hazards and evaluate related risks, and effective risk management. In contrast, QMS is concentrated on compliance in regulations, requirements for satisfying customers' expectations, and requirements. The area involving safety problem has broader meaning than that of the reliability problem. From a system safety prospective, it is necessary to consider not only reliability of component, but also system design, dynamic operational environment, human factors, and organizational factors.

This paper conducted a root cause analysis and risk assessment for MD-11 aircrafts' severe hard/bounced and tail strike landings, in order to verify the important of managing safety risk from the beginning of the aircraft development stage. We have found that the risk of the MD-11 is still at the unacceptable level. Therefore, after an aircraft has been entered into service, it is important to establish a link within the system for the risk to be continually monitored, assessed, mitigated, and controlled in actual operating environment. This safety feature of an aircraft can be a strong source of competitiveness in the global aircraft market. Ultimately, these activities reduce the costs due to direct/indirect correction and/or redesign due to system failures.

This paper suggest that SMS cannot be built overnight, thus SMS should be adopted by the aircraft manufacturing industry in order to obtain the actual safety value and prevent aircraft accidents.

In addition to the aircraft manufacturing industry, SMS can also be adopted in a wide range of other areas, such as private aerospace, unmanned aircraft, small helicopter, in order to effectively manage safety risk and prevent accidents.

References

[1] United States General Accounting Office, *Aviation Safety: Improved Data Quality and Analysis Capabilities Are Needed as FAA Plans a Risk-Based Approach to Safety Oversight*, GAO-10-414. Washington, D.C, May 2010.

[2] Reason, J., *Managing the Risks of Organizational Accidents*, Ashgate Publishing Company, Aldershot, UK, 1997.

[3] Stolzer, A., *QMS (AS9100) and SMS: GAP Comparison*, Embry-Riddle Aeronautical University, 2011

[4] International Civil Aviation Organization, *Annex 19 Safety Management*, First Edition, July 2013.

[5] International Civil Aviation Organization, *Safety Management Manual*, SMM Doc. 9859, Third Edition, 2013.

[6] National Transportation Safety Board: *Aircraft Incident Report, Auxiliary Power Unit Battery Fire, Japan Airlines Boeing 787-8, JA829J, Boston, Massachusetts (January 7, 2013)*, NTSB/AIR-14/01. Washington, D.C, 2014.

[7] Kinnersley, S. and Roelen, A., "The contribution of design to accidents", *Safety Science*, Vol. 45, 2007, pp. 31-36.

[8] Younossi, A., "FAA - Safety Management Systems", *Proceedings of the 2010 ICAO High level Safety Conference*, Mar 29, 2010.

[9] Federal Aviation Administration, *Safety Management System (SMS) Aviation Rulemaking Committee (ARC) SMS ARC Recommendations Final Report*, March 31, 2010.

[10] United States General Accounting Office, *Aviation Safety: Additional Oversight Planning by FAA Could Enhance Safety Risk Management*, GAO-14-516, Washington, D.C, Jun 2014.

[11] Safety Management International Collaboration Group (SM ICG), *The Senior Manager's Role in Safety Management System*, May 2012.

[12] Federal Aviation Administration, *Advisory Circular Safety Management Systems Aviation Service Providers*, AC No. 120-92B, January 8, 2015.

[13] Nation Transportation Safety Board, Investigations [website]. Available at http://www.ntsb.gov/investigations/Pages/default.aspx.

[14] Nation Transportation Safety Board, *Aircraft Accident Report: Inadvertent In-Flight Slat Deployment China Eastern Airlines Flight 583*, Washington, D.C, Oct 27, 1993.

[15] Nation Transportation Safety Board, "*Aircraft Accident Report: Crash during Landing Federal Express, INC. McDonnell Douglas MD-11, Newark International Airport, Newark, New Jersery (July 31, 1997)*", NTSB/AIR-00/02. Washington, DC, 2000.

[16] Shappell, S. and & Wiegmann, D., "Applying Reason: The Human Factors Analysis and Classification System (HFACS)", *Human Factors and Aerospace Safety*, Vol. 1, 2007, pp. 59–86.

[17] Wiegmann, D. and Shappell, S.A., *A Human Error*

Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System, Ashgate Publishing Company, Burlington, VT. 2003.

[18] Australian Transport Safety Bureau, Aviation Research and Analysis Report, *Evaluation of the Human Factors Analysis and Classification System as a predictive model*, AR-2008-036, Dec 2010.

[19] Federal Aviation Administration, *Transport Airplane Risk Assessment Methodology (TARAM) Handbook*, PS-ANM-25-05, Draft Revision 1.

[20] Boeing Commercial Airplanes, *Statistical Summary of Commercial Jet Airplane Accidents Worldwide Operations 1959 – 2013*, Seattle, Washington, Aug 2014.

[21] Federal Aviation Administration, *Manufacturers Safety Management System Pilot Project Report Design and Manufacturing Organizations*, 2012.

[22] Federal Aviation Administration, *A Report from the Part 21/Safety Management System (SMS) Aviation Rulemaking Committee to the Federal Aviation Administration*, Oct 5, 2014.

DOI: http://dx.doi.org/10.5139/IJASS.2015.16.3.451