The House of Integrity: Modern Asset Integrity Management A Process Safety approach

Alejandro C. Torres-Echeverria
Risktec Solutions, Inc.
15810 Park Ten Place, Suite 100, Houston, TX 77084, USA
Alejandro.Torres@risktec.com

Lisa Willnauer
TÜV International GmbH
Am Grauen Stein, 51105 Cologne, Germany
Lisa.Willnauer@de.tuv.com

Steven Saunders
Risktec Solutions, Ltd
Office 3006, Liwa Heights, Jumeirah Towers,
PO Box 450113, Dubai, United Arab Emirates
Steven.Saunders@risktec.com

Prepared for Presentation at
American Institute of Chemical Engineers
2016 Spring Meeting
7th Latin American Conference on Process Safety
Lima, Peru
August 22-23, 2016

The House of Integrity: Modern Asset Integrity Management A Process Safety approach

Alejandro Torres-Echeverria
Risktec Solutions, Inc.
15810 Park Ten Place, Suite 100, Houston, TX 77084, USA
Alejandro.Torres@risktec.com

Lisa Willnauer
TÜV International GmbH
Am Grauen Stein, 51105 Cologne, Germany
Lisa.Willnauer@de.tuv.com

Steven Saunders
Risktec Solutions, Ltd
Office 3006, Liwa Heights, Jumeirah Towers,
PO Box 450113, Dubai, United Arab Emirates
Steven.Saunders@risktec.com

Keywords: Asset integrity, integrity management, process safety management, reliability, maintenance, inspection.

Abstract

Physical Asset Integrity Management (AIM) is a widely known and well-defined process that, if applied in the correct way, can offer asset owners and operators the ability to manage risk and assure the integrity of assets throughout their life cycle. The purpose of physical AIM is for an organization to be able to assert, with confidence and based on the evidence, that their assets are safe and reliable.

The foundation required to build a robust approach to AIM starts with using recognized international standards. ISO 55000 series of standards (formerly PAS 55) sets out good practice requirements for managing physical assets and ensures that consistent terminology is applied. From this foundation an AIM "house" can be built.

This paper introduces a model called the "Asset Integrity Management House". The approach presented here intends to bring together under one roof the disciplines of process safety and physical asset integrity management, supported on reliability foundations, to facilitate the realization of common goals. This is physical asset management focused on risk management towards the reduction of major incident risks.

The model sub-divides into three floors: 1) Physical AIM system. The top floor comprises the system of policies, standards, procedures and resources needed to be in place to deliver integrity over the whole life cycle of an asset. 2) Integrity, reliability and process safety assessment. The middle floor is about conducting the relevant analyses to ensure that integrity risks are understood, the assets are designed and operated to achieve their performance targets, and safety risks are as low as reasonably practicable. 3) Maintenance, inspection and testing. At the ground floor level are the activities which maintain the design intent through life. Spanning all floors is the competence of personnel in performing their tasks to the required standards.

The benefits of such an encompassing simplified model is that each of the different disciplines involved can identify the contribution they are making, and align their processes and work towards achieving a common goal.

1 The need for an integrated model between asset management and process safety management

Asset Integrity can be defined as "the ability of an asset to perform its required function effectively and efficiently whilst protecting health, safety and the environment" [1]. Asset Integrity Management (AIM) offers asset owners and operators the ability to manage risks and assure the integrity of assets throughout their life cycle. The purpose of AIM is to provide an organization a system that ensures consistent and safe performance, being able to keep their assets safe and reliable. PAS 55 [2], which has now evolved into ISO 55001 [3], is an international standard that establishes guidance for management of physical assets. ISO 55001 is actually applicable to any type of assets, although it is intended to be used specifically for managing physical assets.

High hazard industries must maintain a focus on risk management towards reducing the risk of major incidents. OGP 415 [4] is a previous attempt to provide sound guidance in reduction of major incidents risk by focusing on asset integrity management. Reduction of major incidents hazards is actually the main objective of the process safety discipline. Nevertheless, disciplines such as process safety and integrity management are still being treated separately inside many organizations. Reliability, maintenance (these two being fundaments of integrity management), and safety are still being managed as "silos" in some organizations. Silo mentality is an attitude that dominates organizations where different departments do not share information nor work together with other departments of the same organization, which tampers the efforts for achieving common goals in an efficient and cost-effective manner.

The approach presented here brings together under one roof the disciplines of process safety and physical asset integrity management, supported on reliability foundations. This is physical asset management focused on risk management towards the reduction of major incident risks. This is called the "Asset Integrity Management House".

It is worthy to make a distinction between occupational (or personal) safety and process safety. Occupational health and safety is mostly focused on high frequency "low" consequence events (e.g. occupational injuries, like slips, trips, and falls), while process safety is focused on low frequency high consequence events (e.g. those that can have catastrophic consequence, like wide

reaching or multiple fatalities; i.e. major incidents). As OGP 415 states, "good occupational health and safety performance of an asset does not guarantee major incident prevention" [4].

2 The Plan-Do-Check-Act continuous improvement process

The basis of most modern management systems, such as quality (ISO 9001 [5]), environment (ISO 14001 [6]), occupational health & safety (OHSAS 18001 [7]), and risk management (ISO 31000 [8]), are founded on a standard iterative continuous improvement management cycle: Plan, Do, Check, Act. Thus, most management systems share a common structure. As established by HSG 65 [9]:

- Plan. Development of a policy and plans for implementation.
- Do. Implementation and execution of the plan with adequate resources.
- Check. Review and measurement of performance.
- Act. Taking action to act on deviations identified and lessons learned

3 The different approaches and elements

3.1. The approach for process safety

The main focus or process safety is the prevention and control of hazards that have the potential for causing major incidents. Major hazards are those with the potential to cause multiple fatalities, catastrophic environmental damage or significant asset loss (i.e. low frequency, high consequence events). Although process safety pertains to the process industry, its principles, methods and techniques can be applied to a wide spectrum of different high-hazard and other industries.

Process safety-focused management has become an important aspect of loss prevention in the process industry worldwide. Example of important related regulations are the Seveso III Directive (implemented as the COMAH Regulations in the UK [10]), and the OSHA PSM regulation in the United States [11] (which precursor was API 750 [12]). Many other countries have followed implementing their own process safety regulations. Modern process safety management is supported by an overall risk-based strategy founded on a series of different elements (e.g. hazard identification, competence, management of change, etc.) that intend to implement the four main pillars for process safety: commitment to process safety, understanding of hazards and risks, management of risks, and learning from experience. This approach has been called "risk based process safety" (as published by the Center for Chemical Process Safety [13]). A more recent approach has been published by the Energy Institute (EI) as a high level framework for PSM [14]. The four focus areas of this approach are: Process safety leadership, risk identification and assessment, risk management, and review and improvement. Both the CCPS' and EI's schemes share important similarities.

As discussed above, "good occupational health and safety performance of an asset does not guarantee good major incident prevention" [4]. Even if organizations focus on managing successfully personal safety, they may still experience major accidents. This is supported, for

example, by the Baker Report with reference to the Texas City accident when stated as one of its findings that “BP mistakenly used improving personal safety performance (i.e. personal injury rates) as an indication of acceptable process safety performance at its five U.S. refineries; BP’s reliance on this data and inadequate process safety understanding created a false sense of confidence that it was properly addressing process safety risks at those refineries” [15].

3.2. Risk Management

ISO 31000 [8] provides guidelines for a consistent risk management process, helpful to manage risks effectively and efficiently. This is an international standard which guidance can be implemented for any type of risks (financial, strategic, etc.), and it sets out well principles that can be used for major hazards risk management. In addition to the Plan-do-check-act principle, it establishes a risk assessment process that is at the core of the risk management implementation (the “”do” step). This is illustrated in Figure 1.

The process safety risk management process is composed of: establishing the context, risk assessment and risk treatment. Risk assessment consists of performing identification of hazards, followed by a risk analysis (determining the likelihood and consequence of each hazard), and then risk evaluation (comparing the actual risk against corporate risk criteria to determine if this is tolerable or it needs to be further reduced). This makes possible to identify and implement risk control (treatment) measures.

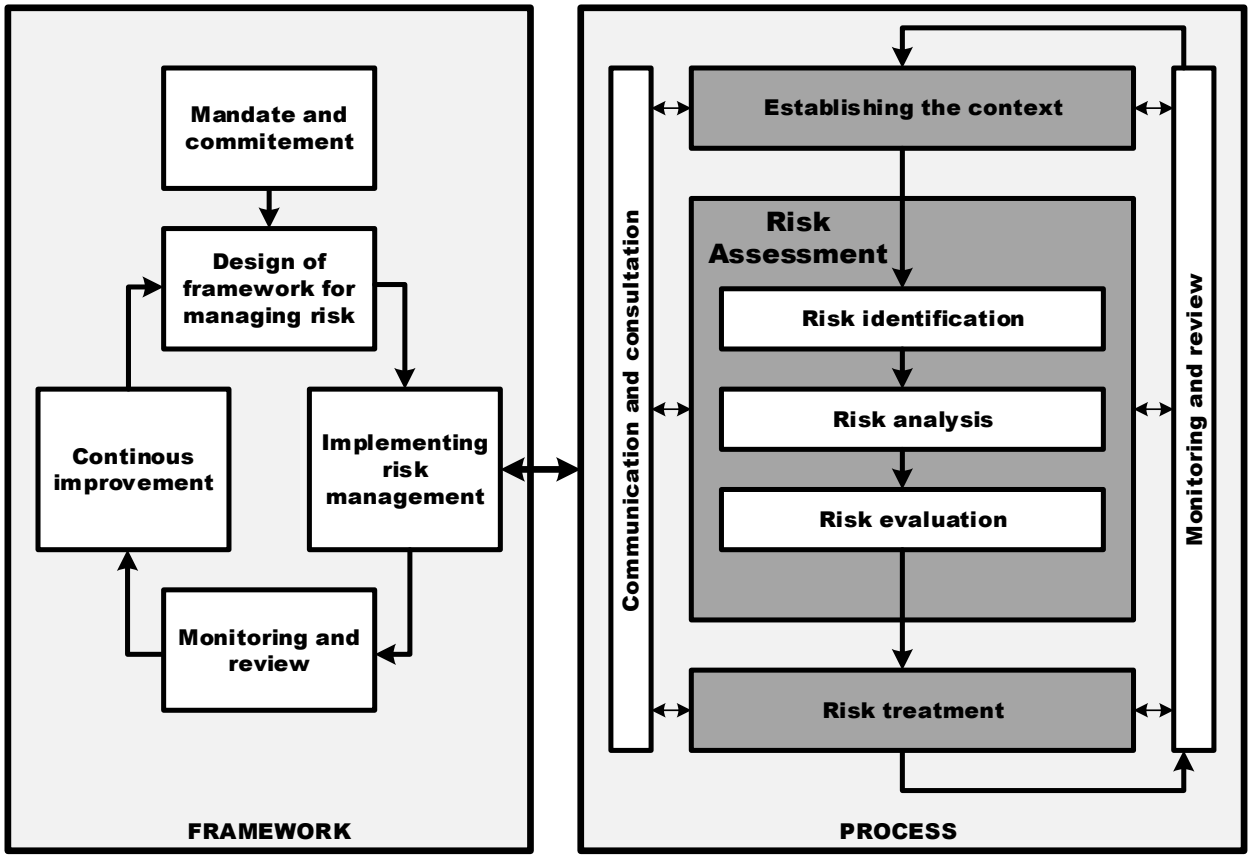

Figure 1. Risk Management framework and process [8]

3.3. Safety critical equipment and performance standards (OGP 415)

A barrier is defined as a functional grouping of safeguards to prevent and control the realization of a hazard [4]. Since barriers can be any measure implemented to support this function, a barrier can be a mix of tangible goods (e.g. equipment) and processes (procedures). Barriers can be preventive (to prevent a hazardous event from taking place), or mitigative (to mitigate the consequences of a hazardous event). Management of hazards is focused on the implementation of barriers for prevention and mitigation.

The interpolation between physical asset management and management of major hazards is realized when certain physical assets become barriers that serve in prevention and control of hazards. Those physical barriers that are critical for safety can be classified as Safety Critical Equipment (SCE). SCE needs to have their performance standards defined in terms of functionality, availability, reliability and survivability [4]. The performance standards determine design specifications and maintenance requirements to maintain their required functionality and integrity throughout their useful life.

3.4. Mechanical integrity and reliability

It becomes clear thus that reliability is at the core of SCE performance standards. Notice that here "reliability" refers to the discipline in charge of analysis and application of techniques to maintain equipment and systems (in this case SCE) performing their intended function and free of failure. Traditionally, mechanical integrity has been a subset of a company's reliability program, encompassing measures and activities intended to ensure the integrity of mechanical equipment through its lifecycle: design, fabrication, installation and operation (mechanical integrity is actually one of the elements of the OSHA PSM regulation [11]). The concept has evolved to encompass all types of critical equipment (not only mechanical), becoming "process and equipment integrity", and subsequently "asset integrity" [13]. This concept of asset integrity primarily involves inspections, tests, preventive and predictive maintenance, repair activities and quality assurance processes to maintain SCEs fit for use.

3.5. The asset integrity management approach (PAS 55 and ISO 55001)

PAS 55 Asset Management [2] is the standard for the optimized management of physical assets. PAS 55 introduced a risk-based management approach for asset integrity, by putting risk assessment and management at the center of the program. Also, notice that several other elements of the asset management structure overlap with those of process safety management; i.e. risk assessment, management of change, incident investigation, etc. Two of the principles of risk management set by PAS 55 are that is has to be 1) risk based, and 2) integrated. PAS also introduced the concept of "critical assets" as those "having the greatest potential to impact on the achievement of the organizational strategic plan". In an interpolation with process safety, assets that are crucial for avoidance of major hazards can be classified as SCEs.

Some of the most relevant contributions of PAS 55 were:

- It structured physical asset management into a standard management system, following the plan-do-check-act principle.
- Establishes as an essential attribute of physical asset management to be risk-based.
- Called for physical asset management to be integrated.
- Introduced several elements that can be easily overlapped with process safety management systems (i.e. the CCPS risk-based process safety [13], or the EI framework on PSM [14] programs) into the physical asset management system; such as risk identification and assessment, contingency planning, training and competence, management of change, physical asset monitoring, audit and management review.

ISO 55001 [3] is the newest international standard for asset management. It is an evolution of PAS 55 (which was actually phased out after the release of ISO 55001). ISO 55001 scope was made wider in comparison with PAS 55, and it is applicable to any type of assets (financial, human, information, etc.), although it is intended to be used mainly for managing physical assets. This wider scope makes its requirements to be more generic. As a result, ISO 55001 addresses risk management with less detail than PAS 55, which guidance was more specific. Regarding risk management, ISO 55001 only requires to determine "actions to address risks and opportunities", with identification and assessment of risks, and to include them into risk management and contingency planning. It actually refers the reader to "see ISO 31000 for further guidance on risk management". Thus, ISO 55001 rather than establishing detailed requirements for the risk management process defers them to the use of ISO 31000, although following ISO 31000 is not made mandatory. It can be said that ISO 55001 is the latest and currently valid approach for asset management, but PAS 55 is still a very useful reference for physical asset management, and it can be used as a complement.

3.6. Correspondence between different approaches

Table 1 presents the correspondence between ISO 55001, PAS 55 and the CCPS' and the EI's process safety management approaches. The table demonstrates how risk-based process safety elements overlap with ISO 55001/PAS 55 physical asset management systems. This is where the integration of physical asset management and process safety can be accomplished; i.e. putting in place a physical asset management system with a focus on major incident risks reduction.

Table 1. Correspondence ISO 55001/PAS 55 to the CCPS Risk Based Process Safety and the EI Process Safety Management

ISO 55001			PAS 55		CCPS RBPS	EI PSM
Section	Element		Element	Notes	Element	Element
4. Context of the organization	4.1. Understanding the organization and its context		4.3.1. AM strategy	Loosely mentioned in ISO 55002 4.1.1		
	4.2. Understanding the needs and expectations of stakeholders				5. Stakeholder outreach	5. Communication via stakeholders
	4.3. Determining the scope of the AM system		4.1. General requirements			
	4.4. AM system		4.1. General requirements			
5. Ledearship	5.1. Leadership and commitment		4.4.1. Structure, authority and responsibilities			1. Leadership commitement and responsibility
	5.2. Policy		4.2. AM policy			
	5.3. Organizational roles, responsibilities and authorities		4.4.1. Structure, authority and responsibilities			
6. Planning	6.1.Actions to address risk and opportunities for the AMS		4.3.3. AM plans			
	6.2. AM objectives and planning	6.2.1. AM objectives	4.3.2. AM objectives			
		6.2.2. Planning to achieve AM objectives	4.3.3. AM plans			
			4.4.7.1. Risk management process	Loosely implicit in 6.2.2, referred to ISO 31000		
			4.4.7.2. Risk management methodology	Loosely implicit in 6.2.2, referred to ISO 31000		
			4.4.7.3. Risk identification and assessment	Mentioned in 6.2.2 (less detailed than PAS55), referred to ISO 31000	7. Hazard identification and risk analysis	6. Hazard identification and risk assessment
			4.4.7.4. Use and maintenace of asset risk information	Loosely mentioned in 6.2.2, referred to ISO 31000		
			4.3.4. Contingency planning	Loosely mentioned in 6.2.2	16. Emergency management	14. Emergency preparedness
7. Support	7.1. Resources		4.5.2. Tools, facilites and equipment			
			4.4.3. Training, awareness and competence			
	7.2. Competence		4.4.3. Training, awareness and competence		3. Process safety competency	3. Employee selection, placement and competency, and health assurance
					12. Training and performance assurance	
	7.3. Awareness		4.4.3. Training, awareness and competence			
	7.4. Communication		4.4.4. Communication, participation and consultation		4. Workforce involvement	4. Workforce involvement
					5. Stakeholder outreach	5. Communication via stakeholders
	7.5. Information requirements		4.4.6. Information management		6. Process knowledge management	7. Documentation, records and knowledge management

AM = Asset Management

Table 1. [Continuation]

ISO 55001			PAS 55		CCPS RBPS	EI PSM
Section	Element		Element	Notes	Element	Element
	7.6. Documented information	7.6.1. Documented information - general	4.4.5. AM system documentation		6. Process knowledge management	7. Documentation, records and knowledge management
		7.6.2. Creating and updating documented information	4.4.5. AM system documentation			
		7.6.3. Control of documented information	4.4.5. AM system documentation			
8. Operation	8.1. Operational planning and control		4.5.1. Lifecycle activities (very loosely)		8. Operating procedures	
					9. Safe work practices	8. Operating manuals and procedures
						17. Work control, permit to work and task risk management
					14. Operational readiness	9. Process and operational status monitoring, and handover
					15. Conduct of operations	13. Operational readiness and process startup
						10. Management of operational interfaces
	8.2. Management of change		4.4.9. Management of change		13. Management of change	12. Management of change and project management
	8.3. Outsorcing		4.4.2. Outsorcing of AM activities		11. Contractor management	18. Contactor and supplier selection and management
9. Performance evaluation	9.1. Monitoring, measurement, analysis and evaluation		4.6.1. Performance and condition monitoring		18. Measurement and metrics	15. Inspection and maintenance
	9.2. Internal audit		4.6.4. Audit		19. Auditing	20. Audit, assurance, management review and intervention
	9.3. Management review		4.7. Management review		20. Management review and continuous improvement	20. Audit, assurance, management review and intervention
10. Improvement	10.1. Nonconformity and corrective action		4.6.5.1. Corrective and preventative action		10. Asset integrity and reliability	15. Inspection and maintenance
	10.2. Preventive action		4.6.5.1. Corrective and preventative action		10. Asset integrity and reliability	15. Inspection and maintenance
	10.3. Continual improvement		4.6.5.2. Continual improvement		20. Management review and continuous improvement	
			4.4.8. Legal and other requirements	References scattered in several clauses in ISO 55001	2. Compliance with standandards	2. Identification and compliance with legislation and industry standards
			4.6.2. Investigation of asset-related failures, incidents and nonconformities	Subjectively suggested in ISO 55001 clause 10.1 (some guidance in ISO 55002 10.1.20)	17. Incident investigation	19. Incident reporting and investigation
			4.6.3. Evaluation of compliance	Loosely scattered in several clauses in ISO 55001		
			4.6.6. Records	Not covered explicitly, although can be implicit in ISO 55001 clause 7.6.3		
					1. Process safety culture	
						16. Management of safety critical devices

AM = Asset Management

4 Integration of the model

This section presents the integration of the different approaches and elements into one single Physical Asset Integrity model named the "Asset Integrity Management House", which is illustrated in Figure 2. The model is sub-divided into three floors, described in the next sub-sections. The model integrates under one roof the disciplines of physical asset integrity and process safety management, supported on reliability foundations, and it is developed down to elementary methodologies and techniques that facilitate its successful implementation.

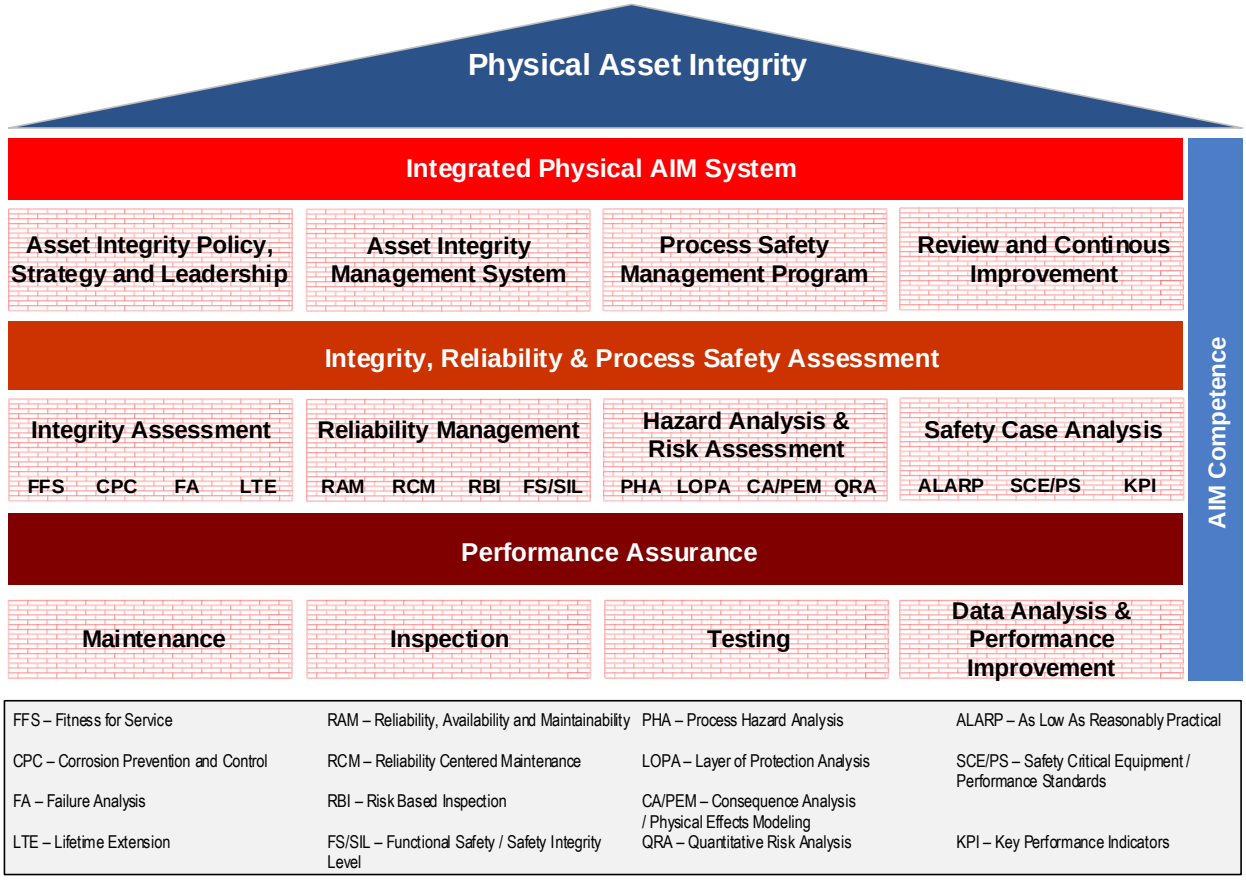

Figure 2. The Physical Asset Integrity Management House

4.1. Integrated Physical AIM System

The first level of the model is composed of four components. The two key components are the Asset Integrity management system and the Process Safety management system. Both management systems are integrated, especially in the elements where they converge (i.e. where some elements of ISO 55001/PAS 55 overlap those of the CCPS Risk Based Process Safety and/or the EI Process Safety Management programs, as per Table 1). The other two components:

Asset integrity policy, strategy and leadership, and Review and continuous improvement are foundations over which those two management systems are implemented. "Using an integrated management systems approach allows a management system to be built on elements of other management systems, such as for quality, environment, health and safety, and risk management. This can improve integration across different disciplines and improve cross-functional coordination" [16].

a) Asset Integrity policy, strategy and leadership. A policy is a high level document that establishes the organization's intentions and direction. A strategy is a plan of action directed towards achievement of the organization goals and objectives. This needs to be aligned with the organization's strategic plan [2]. Finally, leadership is essential to steer the organization towards successful implementation of the management system and achievement of its objectives. It sets commitment and accountability of directors and managers, which are critical for success of any safety management system, and facilitates involvement at all levels of the organization. Leadership is the foundation of an adequate safety culture within an organization, since "top management should create the vision and values that guide policy, practice and actively promote these values inside and outside the organization" [17].
b) Asset Integrity management system. It is the combination of policy, strategy, objectives, plans, activities, processes and organizational structures needed for the implementation and sustenance of the integrity of the organization's assets [2]. In the context of this paper, it is based on ISO 55001 [3] and PAS 55 [2], supported by ISO 31000 [8].
c) Process Safety management (PSM) program. The PSM program integrates management practices, procedures and technologies intended to prevent or minimize the consequences of catastrophic incidents related to the release of toxic, reactive, flammable or explosive chemicals. In the context of this paper, is based on the PSM framework set by CCPS [13] and IE [14].
d) Review and continuous improvement. These implement the CCPS' "learn from experience" pillar [13]. It is basically the measurement and performance assessment of the management system and the physical assets themselves, with the aim of implementing continuous improvement. It includes elements such as incident investigation, performance metrics, audit, management review, and continuous improvement.

4.2. Integrity, Reliability & Process Safety Assessment

e) Integrity Assessment. This part provides the assessment and follow up of processes traditionally assigned to physical asset integrity management. Traditionally these processes pertained to mechanical integrity, but have evolved to encompass all types of physical assets.
    - Fitness for Service – FSS. A FFS assessment is a quantitative evaluation performed to evaluate the structural integrity of a piece of equipment or a component that is in service and which is sustaining a flaw or damage. Guidance can be found in API 579 [18]. FFS assessments can encompass several damage mechanisms, such as fracture, fatigue, cracks, corrosion, etc.

- Corrosion Prevention and Control – CPC. Corrosion is the deterioration of material or its properties due reaction with its chemical environment. A CPC program includes activities for prevention and control of corrosion, and it can encompass all phases of the lifecycle. It applies management principles, engineering design and analysis, quality assurance, technologies and processes for tracking, control and repair of corrosion problems [19]. This may include for example materials selection, protective coating, inhibitors, environmental control, corrosion allowances and cathodic protection. In the operation phase this includes corrosion monitoring and control measures.
- Failure Analysis – FA. Failure relates to loss of functionality, which can be gradual or sudden. Failure analysis is the process of examination of a failed system or component, using engineering data collection and analysis techniques, to determine the damage mechanisms and the immediate and root causes of a failure. Failure analysis can range from a simple desktop analysis to a comprehensive failure investigation. Some of the specialized techniques that can be used are Failure Modes and Effect Analysis (FMEA), Fault Tree Analysis, and other multiple testing and forensic engineering techniques. Failure Analysis is part of the "learning from experience" pillar, and can be a part of the incident investigation element. Results from failure analysis are used for prevention of further failures and control of failure consequences.
- Lifetime Extension – LTE. This is a program that can be implemented to extend the life of ageing assets (equipment and facilities) beyond the original design expected lifetime. Lifetime extension is based on a rigorous condition assessment and gap analysis of regulatory requirements [20], and subsequent periodic monitoring, review and evaluation (integrity, functionality, performance, safety). Lifetime extension decisions for safety critical equipment needs to be based on an adequate risk assessment (see [21]).

f) Reliability management. This deals with assessment, monitoring and assurance of asset dependability. Reliability is a wide concept that can be sometimes confusing. Here the concept refers to the discipline of reliability engineering. Reliability of an asset can be quantified using several measures, one of them is actually called "reliability". Thus, the concept of dependability can be used as a collective term to describe an asset's attributes of reliability, availability and maintainability (RAM), i.e. the "trustworthiness" of an asset to keep delivering its service free of failure.
   - Reliability, Availability, Maintainability – RAM. RAM analysis can encompass several different types of studies to determine system dependability. In its more common form it is actually a study of system availability. Reliability is the probability of a system keeping performing its intended function (i.e. to stay free of failure) during a specific period of time. Maintainability is the probability of a system being repairable (at a given time). Availability is a measure that combines reliability and maintainability, to quantify the probability of a system being capable of performing its intended function (i.e. to be available) at a given time. For example, a system may be free of failure (reliable) but unavailable due to maintenance. Thus,

availability quantifies all time down (either by failure or by maintenance) to predict the fraction of time that the system will be running.

- Reliability Centered Maintenance – RCM. RCM guides the design of maintenance strategies based on analysis for optimization of maintenance costs against asset availability; i.e. maximization of availability and minimizations of costs. Thus, RCM is used to define the optimal maintenance strategy is terms of, for example, replacement intervals, spares holding, proof-test intervals and condition monitoring [22]. RCM integrates FMECA, probabilistic safety analysis, preventive maintenance, predictive testing and inspection, repairs and proactive maintenance [23, 24]. RCM is usually focused on critical assets. In the case of safety barriers, those are part of the facility's SCE. Thus, maintenance strategies optimized by RCM must consider availability and risk (safety); this becomes what is now called Reliability and Risk Centered Maintenance [25]. A guide to RCM can be found in IEC 60300-3-11 [26].
- Risk Based Inspection – RBI. This is the development of inspection plans (equipment identification, scheduling and techniques selection) for critical equipment based on the results of risk analysis, in lieu of time-based or prescriptive planned inspection. A standard for RBI is API 580/581 [27, 28]. RBI has been traditionally developed for mechanical pressurized equipment, although the concept and overall methodology can be extended to other types of physical assets. RBI can be used as feedback to a FFS assessment and risk re-assessment. RBI also overlaps with condition-based monitoring.
- Functional Safety / Safety Integrity Level – FS/SIL. Functional Safety refers to safety achieved by means of the correct operation of a system or equipment. An important share of safety critical systems in the process industries are electrical, electronic and programmable electronic systems (E/E/PE). IEC 61508 [29] addresses design and implementation of E/E/PE safety-related systems. The standard is generic, applicable to any type of industry. Some of the industry-specific standards derived from IEC 61508 are IEC 61511 [30] for process industry and IEC 61513 [31] for nuclear industry. E/E/EP safety-related systems are called Safety Instrumented Systems (SIS) in the process industry. Some examples of E/E/EP safety-related systems are emergency shutdown systems, fire & gas detection systems and alarm systems. The two most important contributions of the IEC standards are the establishment of the safety lifecycle for SIS and the definition of Safety Integrity Levels (SIL). The SIL is a discrete measure of performance (ranging from 1 to 4) based on the maximum acceptable probability of failure of a SIS. Maintenance of a specific SIL level depends on the reliability of the system components as well as periodic proof testing of the system. Therefore, functional safety needs to be sustained by appropriate reliability modeling and management. Functional safety is one important example where safety and reliability management overlap.

g) Hazard Analysis & Risk Assessment. Risk management, and more specifically the risk assessment process is based on analysis of two main concepts: the identification of hazards and the analysis and evaluation of risk (see Fig. 1). Hazard is defined as characteristic or condition that has the potential to cause harm (to people, the environment or the assets). Risk

is defined as the combination of likelihood and the potential level of consequences of a hazardous event.

- Process Hazards Analysis – PHA. Hazard identification is the foundation of the risk assessment process. Errors in this step are carried over the entire risk management process, since hazards that are not identified cannot be evaluated and treated. Process Hazards Analysis (PHA) is a generic name for hazard identification. There are several well established PHA techniques, such as HAZID, HAZOP, FMEA, etc., which can be selected according to several factors, such as project lifecycle stage and purpose of the PHA. One of the best guides for PHA is CCPS [32].
- Layer of Protection Analysis – LOPA. This is a simplified semi-quantitative risk analysis methodology. The most comprehensive description of LOPA can be found in CCPS [33]. The LOPA method allows identification of the likelihood of a loss event taking into account the layers of protection (barriers) available, and to determine if the residual risk is tolerable or it needs further reduction. This method is widely used for SIL selection.
- Consequence Analyses / Physical Effects Modeling – CA/PEM. Consequence analysis is the study of the potential outcomes and their severity of a hazardous event. CCPS [34] provides a good summary of CA in the process industry. CA starts by definition of an incident. Subsequently a source model is applied to have a physical description the release process of material (loss of containment), which includes quantity, rate and chemical phase of the discharge. A dispersion model is then utilized to understand how the released material travels and disperses in the surrounding environment. This provides quantification of the reach of a toxic or flammable release (the hazard endpoint). If the release is flammable, a fire or explosion model can be used to "convert the source model information on the release into energy hazard potentials such as thermal radiation and explosion overpressures" [34]. Finally, effect models translate the potential effects on people, assets and/or environment. All this is a comprehensive process named Physical Effects Modelling (PEM). There are other simplified methodologies to address consequence analysis, but PEM is the more detailed and comprehensive modality.
- Quantitative Risk Analysis – QRA. A fully quantitative methodology intended to obtain a numerical estimation of risk: incident likelihood and consequence severity. Consequence severity is addressed using CA/PEM described above. The second part, frequency (likelihood) analysis, is addressed using reliability engineering techniques, such as parts count, Fault Tree Analysis, Event Tree Analysis, etc. Once both risk components are estimated, the actual risk is compared against corporate risk criteria to determine if the risk level is tolerable or needs further reduction (i.e. risk evaluation), which completes the risk assessment. Guidance can be found in [34].

h) Safety Case Analysis. A safety case is a document that demonstrate how hazards and risks related to operation of a specific facility are identified and managed. In some regions they are called a HSE case. Safety cases for high-hazard industries are required by law in some regions or countries (e.g. Seveso III in Europe, COMAH in the UK, Australia's Management of Safety on Offshore Facilities). Also, some major operators in some industries apply a

safety case requirement because of their benefits. Specific sectors in some other countries, such the US Nuclear Regulatory Commission, have similar regulations that require a Safety Analysis Report (10 CFR 50.71(e) [35]).

An HSE case is operation-specific. It is focused on major incident hazards and should demonstrate that risks are managed to a level As Low as Reasonably Practicable (ALARP). A Safety Case encompasses HSE management systems, hazard identification and risk assessment processes, risk reduction (mitigation and control) measures (e.g. SCEs), ALARP demonstration and remedial action plans. It is therefore an all-encompassing document related to management of major incident hazards. Safety cases have a goal setting approach that fosters continuous improvement.

The analysis required to integrate a safety case, and subsequent analysis of the safety case itself, provides a template for assurance of major hazards management with focus on safety critical equipment. Thus, the safety case can be used both a as tool and a source of information. A safety case might seem redundant if a good HSE management system is in place, but the safety case allows integration of the management system with plant operations in order to ensure that risks are managed to ALARP. Therefore, the safety case provide cohesion between the management systems' spirit and its implementation. Besides hazard analysis and risk assessment, there are three key elements of the safety case that are directly relevant to physical asset integrity management: ALARP demonstration, SCE identification and assessment, and performance indicators.

- As Low as Reasonable Practicable – ALARP. The main aim of a safety case is to demonstrate that risks have been reduced to an ALARP level. Demonstration of ALARP is the HSE's [36] approach to compliance with COMAH regulations requirement to reduce risks so far as reasonably practicable in the UK [37]. Many high hazard industries operators and sectors in other countries have adopted ALARP demonstration (or similar concepts, such as SFAIRP, ALARA) as an internal regulation. ALARP demonstration is a balance between the risk level to be avoided, the effort (time, difficulty and cost) to achieve risk reduction, and the residual risk, based on the concept of "gross disproportion". ALARP demonstration requires account of implementation of risk reduction measures, for example using SCE. Thus, ALARP demonstration is closely linked to the identification and implementation of SCE and definition of their performance standards.
- Safety Critical Equipment and Performance Standards – SCE/PS. When addressing hazard identification and risk assessment, the safety case focuses on identification and analysis of Safety Critical Equipment (i.e. key critical safety barriers). The failure of SCE items "could cause or contribute to a major accident" [1]. Performance standards are developed in order to be able to understand their function, set measures of required performance and measure their effectiveness. All SCE items need to have an impairment risk assessment, either embedded in the overall risk assessment or separately. Finally, SCE items need to have a verification scheme.
- Key Performance Indicators – KPIs. These are leading and lagging indicators that allow monitoring progress and maintenance of physical assets integrity with respect to safety, providing "dual assurance" that key risk control systems (SCEs) are operating as intended [38]. They provide assurance that SCE items are being properly

maintained, a measurement of performance of risk controls' effectiveness and if risks are being adequately controlled, as well as indication of developing issues that might need attention and early warning of SCE deterioration before catastrophic failure [38]. Leading indicators may include, for example, number of functional tests completed on time and SCE items found in fully compliance with codes and standards [4]. Lagging indicators for instance could be spurious trips and SCE failure rates. KPIs can be set at facility level and at equipment level. Good guidance in KPIs can be found in OGP 456 [39] and API 754 [40].

4.3. Performance Assurance

In the context of this article, physical asset performance assurance is composed of the basic activities at the ground floor level that maintain the design intent through life: Maintenance, inspection and testing. Analysis of the results of those activities are used to identify potential issues and improvement opportunities.

i) Maintenance. This is the performance of tasks to maintain the functional capability (and safety) of equipment and systems [41]. Preventive maintenance is made of inspection and/or servicing task that have been preplanned to retain functionality of operating equipment, while corrective maintenance is the performance of unplanned tasks to restore the functionality of malfunctioning equipment [41].
j) Inspection. The examination of a piece of equipment or item to determine their condition using visual surveys and various non-destructive testing (NDT) techniques.
k) Testing. A physical intervention of an item to verify that functionality, performance or integrity has been achieved and is maintained as specified. It includes NDT techniques, overlapping with the inspection function. A category of testing that is of special interest for SCE is proof testing, which primary objective is to detect dangerous unrevealed failures, especially in dormant or standby safety systems (e.g. systems that actuate only on demand, like some fire detection or emergency shutdown systems).
l) Data Analysis and Performance Improvement. This embraces the collection, processing and analysis of data with the objective of identifying potential issues and opportunities for improvement. It is a fundamental function of asset integrity management.

4.4. Competence

Competence of the people involved at any stage or activity of the physical asset integrity management is fundamental. Organizations are made of people, and the quality of their personnel determines the organization performance at all levels. Competence of people includes education, training and experience. A fourth dimension can also be fitness for work. Sustained competence of people is ensured by appropriate selection and recruitment, training, development programs, and competence reviews.

4.5. Summary

It can be noticed that the core of the model for management of physical asset integrity is accomplished by the integration of the disciplines of integrity assurance, reliability management, process safety and risk, all of them within the framework of management. This is illustrated in Figure 3.

Figure 3. Integration of disciplines for Physical Asset Integrity Management

5 Conclusions

This paper presented a model called the "Asset Integrity Management House", which brings together under one roof the disciplines of process safety and physical asset integrity management, supported on reliability foundations. With this model, physical asset management is focused on risk management and towards the reduction of major incident risks. This is an approach based on process safety, which can be extrapolated to other major hazard industries.

6 References

[1] HSE, 2007. Key Programme 3. Asset Integrity Program. Health and Safety Executive, Hazardous Installation Directorate, Offshore Division. Her Majesty Stationery Office, Norwich, UK.

[2] BSI, 2008. PAS 55-1:2008 Part 1: specification for the optimized management of physical assets. British Standard Institution, London, UK.

[3] ISO, 2014. ISO 55001. Asset management – Management systems – Requirements. International Organization for Standardization, Geneva, Switzerland.

[4] OGP, 2008. OGP 415 Asset integrity – the key to managing major incident risks. International Association of Oil & Gas Producers, London, UK.

[5] ISO, 2008. ISO 9001 Quality Management Systems – Requirements. International Organization for Standardization, Geneva, Switzerland.

[6] ISO, 2004. ISO 14001 Environmental management systems – requirements with guidance for use. International Organization for Standardization, Geneva, Switzerland.

[7] BSI, 2007. OHSAS 18001 Occupational Health and Safety Management Systems Requirements. British Standard Institution, London, UK.

[8] ISO, 2009. ISO 31000 Risk management – Principles and guidelines. International Organization for Standardization, Geneva, Switzerland.

[9] HSE, 2013. HSG 65 Managing for health and safety. 3rd ed. Health and Safety Executive. Her Majesty Stationery Office, Norwich, UK.

[10] HSE, 2015. The Control of Major Accident Hazards Regulations. Guidance on regulations. Health and Safety Executive. Her Majesty Stationery Office, Norwich, UK.

[11] OSHA, 1992. 29 CFR §1910.119, Process Safety Management of Highly Hazardous Chemicals. Occupational Safety and Health Administration, US Government Printing Office e-CFR, 2016 Edition, USA.

[12] API, 1990. API RP 750 Management of Process Hazards. American Petroleum Institute, Washington DC, USA.

[13] CCPS, 2007. Guidelines for risk based process safety. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York City, New York, USA.

[14] Energy Institute, 2010. High level framework for process safety management. Energy Institute, London, UK.

[15] Baker III J.A., et. al., 2007. The report of the BP U.S. Refineries Independent Safety Review Panel. The BP U.S. Refineries Independent Safety Review Panel, USA.

[16] ISO, 2014. ISO 55002. Asset management – Management systems – Guidelines for the application of ISO 55001. International Organization for Standardization, Geneva, Switzerland.

[17] ISO, 2014. ISO 55000. Asset management – Management systems – Overview, principles and terminology. International Organization for Standardization, Geneva, Switzerland.

[18] API, 2000. API RP 579 Fitness for Service. American Petroleum Institute, Washington DC, USA.

[19] DoD, 2014. Corrosion Prevention and Control Planning Guidebook for Military Systems and Equipment. Department of Defense, Washington DC, USA.

[20] Cavendra F. and Houari M., 2013. Plant Screening for Ageing Impact in the Process Industry. Chemical Engineering Transactions, 2013, Vol 31: 2013.

[21] NOGA, 2012. Recommended guidelines for the assessment and documentation of service life extension of facilities. Norwegian Oil and Gas Association, Stavanger, Norway.

[22] Smith D.J., 2001. Reliability, maintainability and risk. Practical methods for engineers, 6th ed. Butterworth-Heinemann, Oxford, UK.

[23] NASA, 2008. Reliability-centered maintenance guide for facilities and collateral equipment. National Aeronautics Aerospace Administration, Washington DC, USA.

[24] IAEA, 2007. IAEA-TECDOC-1590 Application of Reliability Centred Maintenance to Optimize Operation and Maintenance in Nuclear Power Plants. International Atomic Energy Industry, Vienna, Austria.

[25] Selvik T.J., Aven T., 2010. A framework for reliability and risk centered maintenance. Reliability Engineering and System Safety, 2010. 96(2): 324-331.

[26] IEC, 2009. IEC 60300-3-11 Dependability management – Par 3-11: Application guide – Reliability centred maintenance. International Electrotechnical Commission. Geneva, Switzerland.

[27] API, 2002. API RP 580 Risk-based Inspection. American Petroleum Institute, Washington DC, USA.

[28] API, 2000. API RP 581 Risk-based Inspection Base Resource Document. American Petroleum Institute, Washington DC, USA.

[29] IEC, 2010. IEC 61508 Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related systems, Parts 1-7, 2nd Edition. International Electrotechnical Commission, Geneva, Switzerland.

[30] IEC, 2003. IEC 61511 Functional Safety - Safety Instrumented systems for the Process Industry Sector - Part 1: Framework, definitions, system, hardware and software requirements. International Electrotechnical Commission. Geneva, Switzerland.

[31] IEC, 2011. IEC 61513 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. International Electrotechnical Commission. Geneva, Switzerland.

[32] CCPS, 2008. Guidelines for Hazard Evaluation Procedures, 3rd ed. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York City, New York, USA.

[33] CCPS, 2001. Layer of Protection Analysis. Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York City, New York, USA.

[34] CCPS, 2000 Guidelines for Chemical Process Quantitative Risk Analysis, 2nd ed. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York City, New York, USA.

[35] NRC, 1982. 10 CFR 50.71 Domestic licensing of production and utilization facilities. Maintenance of records, making or reports. Nuclear Regulatory Commission, US Government Printing Office e-CFR, 2016 Edition, USA.

[36] HSE, 2001. Reducing risk protecting people. Health and Safety Executive. Her Majesty Stationery Office, Norwich, UK.

[37] Ellis G., 2003. The ongoing challenge of demonstrating ALARP in COMAH safety reports. Institute of Chemical Engineers Symposium Series 149, pp103-115. Rugby, UK. Available online at https://www.icheme.org.

[38] HSE, 2006. Developing Process Safety Indicators. A step-by-step guide for chemical and major hazard industries. Health and Safety Executive. Her Majesty Stationery Office, Norwich, UK.

[39] OGP, 2011. OGP 456 Process Safety – Recommended Practice on Key Performance indicators. International Association of Oil & Gas Producers, London, UK.

[40] API, 2010. API RP 754 Process Safety Indicators for the Refinery and Petrochemical Industries. American Petroleum Institute, Washington DC, USA.

[41] Smith A.M., Hinchcliffe G.R., 2004. RCM - Gateway to world class maintenance. Elsevier Butterworth-Heinemann, Oxford, UK.