Risky Business: Functional Safety at Origin

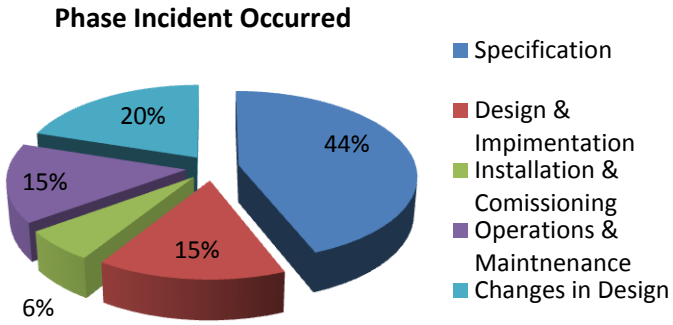
Peter Todd, Engineering Manager, Origin Upstream

No, this is not a review of the 1983 American teen comedy starring Tom Cruise but a brief overview of the serious subject of process functional safety.

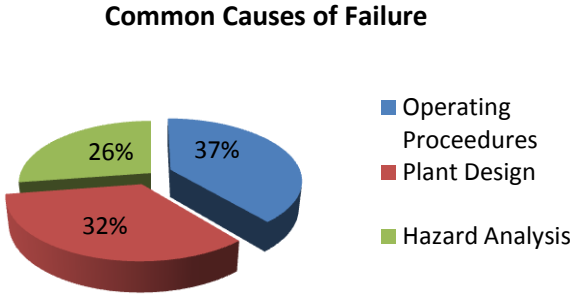
There are significant differences in the legislative frameworks both domestically and internationally under which Origin operate. Legal framework objectives are generally to prevent and minimise the effects of major accidents and near misses. As an operator, legal compliance requirements are often exceeded by adopting performance based standards. One such standard is IEC61511. In order to manage Risk it is useful to understand where errors can occur.

Hindsight is always twenty-twenty

So where are the risks? The UK Health and Safety Executive published findings of 34 accidents that were as a direct result of Safety Systems Failures.



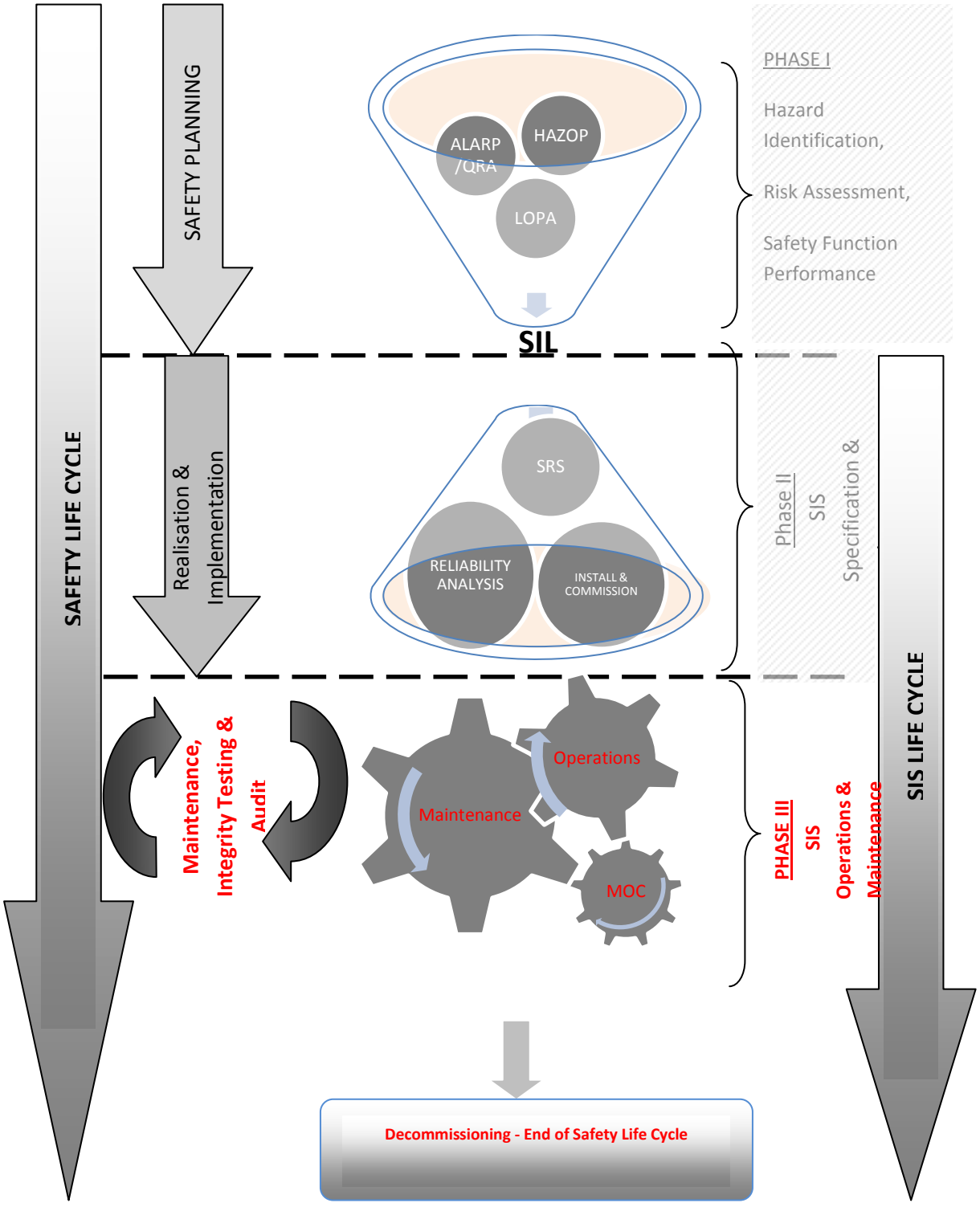
The study concluded that accidents are primarily the result of poor decisions during the various phases of a plant's life (design, installation & commissioning, operation, and maintenance), but that the **majority can be traced to errors related to design**. The study also found that a significant percentage of incidents were caused by changes made after commissioning (20%), as well as errors during operation and maintenance (15%). A subsequent study on accidents in the chemical sector found that three most common causes of failure were errors in operating procedures (37%), in plant design (32%), and in hazard analysis (26%).



We need to look at how risk is specified before we can ensure the best safety systems are designed, operated and maintained in order to mitigate risk low levels.

Foresight is a little more difficult

In order to reduce the likelihood of errors, the Safety Instrumented System (SIS) standard IEC 61511, defines a Safety Life Cycle framework incorporating safety planning, design, realisation of operating and maintenance performance requirements. By adopting a rigorous Quality Plan approach to safety the need for foresight is almost eliminated.



The safety life cycle approach defines performance requirements of organisations, systems, equipment and people from initial concept through to development, detailed design, the engineering and supply of hardware, coding of software, operations and maintenance regimes. This reduces the likelihood of errors and ensures that the Safety Instrumented System (SIS) performs the relevant Safety Instrumented Function (SIF) to the required Safety Integrity Level (SIL) demanded by the Safety Requirements Specification (SRS).

At a people level, individuals involved throughout the Safety Life Cycle are required to be competent. Competency is no accident; it is a requirement of the IEC61511 standard. At a business level, organisations operate rigorous hazard identification and qualification procedures to characterise the SIS. At the component and software level of the SIS equipment, major automation contractors and manufacturers ensure equipment is designed, engineered, coded and built to meet IEC61508 standards.

Substantial improvements in safety performance and operating efficiencies can be realised if the SIS and associated Safety Instrumented Functions (SIFs) are properly engineered and maintained at the right frequency. Maintenance and testing can take place too infrequently for system status to be accurately monitored, or it is performed unnecessarily, which opens the door to human errors that can cause the system to fail. Additionally, the lack of reliability data has lead to unnecessary engineering of SIS, which can also lead to system failure.

The Implementation Challenge

Industry discussions tend to focus on the technical aspects of IEC61511 however project execution, SIS operations and maintenance are proving to have an equal or perhaps greater impact on the quality and success of an IEC 61511 project.

A project may take several years to deliver the required outcome, however the asset may operate over several decades. Both challenges are driving the need for Operating Companies (OC's) to modify and create their internal Project Execution Plans (PEP), tools, guidelines, standards and procedures to ensure asset integrity. The same is true for Engineering, Procurement and Construction (EPC) and MAC.

Safety instrumented systems are vital assets because they protect lives, processes and equipment, but the systems themselves also need protection through performance monitoring throughout their design life. SIS monitoring addresses weakness by collecting necessary, meaningful data and giving engineers the tools they need to act on it.

Investment in resources and assets ensure that risk is correctly identified and systems are appropriately engineered, operated and maintained in order to consistently and continually deliver the safety levels of performance demanded in Origin's operations of today and tomorrow. Safety is no accident!