Caravel

LEADING THE WAY IN PROJECTS

Safety Critical Projects

Caravel Group - for projects that allow no room for error

THE SPECIALIST FOR LARGE COMPLEX MULTI-DISCIPLINED PROJECTS

When Failure is Not an Option

Systems are generally expected to be dependable and solid; none more so, than those that underpin safety critical infrastructure. They are often vital for the common good, however their failure can have catastrophic consequences.

In order to perform safety critical control functions, these systems usually rely on a technology solution as well as a human element. As such, they also carry within themselves the potential for failure, through technology as well as through human error. Failure of one or both of these aspects can lead to incidents and accidents, often threatening life and property on a mass scale.

Any system development or organisational change that is implemented within such an environment is considered a Safety Critical Project - one of the most challenging types of project that an organisation may face or undertake.

Safety Critical Projects are usually found in infrastructure-related industries such as:

- Transport (maritime, rail, road, aviation)
- Utilities (electricity, water & waste, gas, telecommunications)
- Process industries (particularly petrochemical)
- Mining industry
- Emergency services (control rooms etc.)

The risks are many and various and may lie with the owners of the system or equipment, and impact those that pay to use the services delivered by the system or equipment, or those that operate the system or equipment.

Safe systems

Quality systems are often synonymous with minimal re-work. In the same vein, a safe system is also considered to be the most efficient and effective. This is borne out by engineers' efforts to minimise any downtime of equipment and staff (due to illness or injury) while increasing the availability of services to customers.

Safety Critical Projects are usually executed in a distinctly multi-faceted environment and have to address a number of factors. For project managers it means that they deal with complex projects that are further complicated by onerous compliance requirements and conditions.

As a result, Safety Critical Projects share a mix of the following attributes:

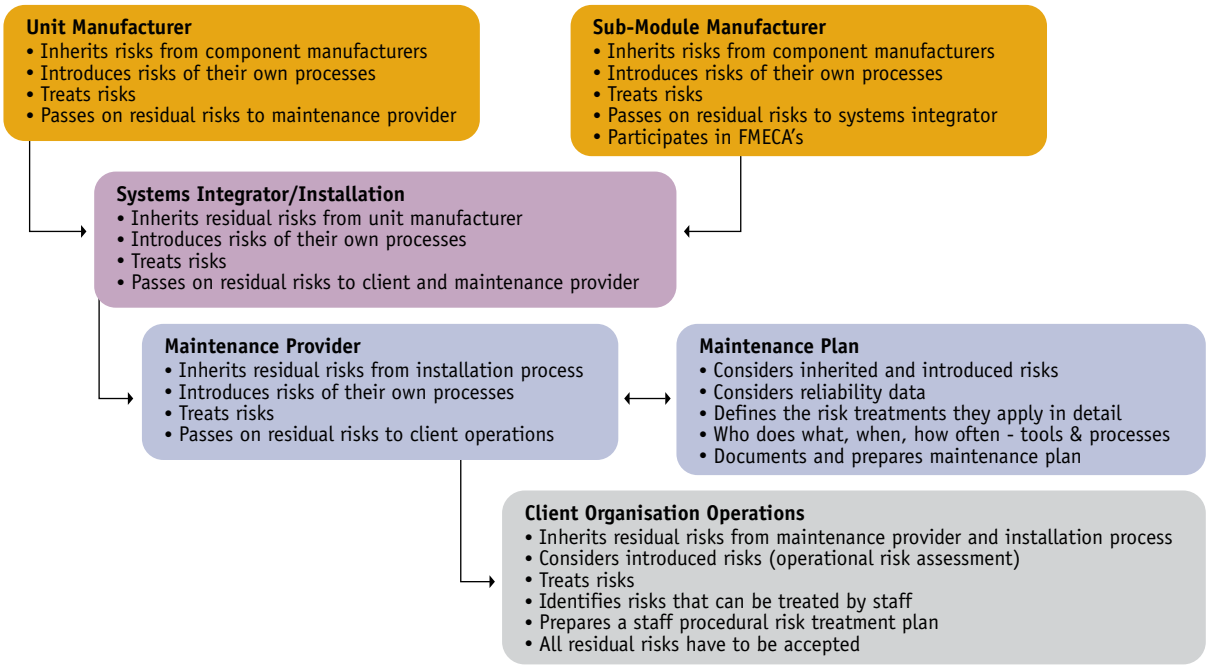
- Industrial electronics development, modification or off-the-shelf supply
- Software development or modification including embedded systems
- Systems integration and implementation
- Business process innovation to accommodate the new technology
- Change implementation to manage the transition from old to new
- Support systems implementation or modification to accommodate the new systems
- Risk management programme including on-going or in-service risk performance monitoring

The Lay of the Land

The framework that surrounds Safety Critical Projects is largely defined by a multitude of complex factors which impact on the project climate and demand experienced project management leadership. These factors are critical project parameters and significantly increase the project complexity, yet they are often misunderstood or inadequately considered.

Safety engineering and risk management

Safety engineering and risk management is at the core of Safety Critical Projects. It is used to identify and treat risks by way of engineering (technology) or processes (human aspects). Risks may also be inherited or introduced through a supplier, and then treated. Residual risks at one level are then transferred to another level in the operational chain.



The flow diagram affords an overview of inherited and introduced risks from components and subsystems to the integrated system.

Technical complexities

Challenges related to the technical environment are often underestimated or overlooked altogether. When systems need to be retrofitted and integrated within existing systems, it inevitably results in a host of technical and operational complexities.

The same also applies for routine maintenance tasks and any other activities carried out at the point of interface between the new and existing systems. All of this can potentially represent a threat to the existing system.

Adapting to changed environments

The deployment of systems within an existing operating environment demands considerable training of employees/operators to ensure that they adapt to the new operational situation. This is vital as incomplete or inaccurate operator training can introduce significant transition risks of incidents or accidents.

The project also has to consider commercial implications when the introduction of new systems interrupts the continuity of the service delivery or imposes a temporary capacity constraint on existing services.

The stakeholder factor

Safety Critical Projects typically operate within a multi-stakeholder environment comprising customers/service users, operators, regulators and/or government authorities. As a result, the project scope tends to be multi-organisational, which further increases the project complexity and calls for a skillful and experienced project management approach.

The legal imperative

The importance of compliance with legal obligations cannot be overstated. Safety Critical Projects have to fulfill stringent legal obligations and must comply with various legislative acts pertaining to the relevant industry. Non-compliance can result in severe penalties for companies and individuals alike.

It is therefore vital, that the legislative environment, as it applies for the particular country and state, is carefully addressed. This includes relevant acts relating to employee safety (Occupational Health and Safety) and public safety (Safety Act).

Likewise, project managers must have a thorough understanding of the legal obligations pertaining to the project. Worst-case scenarios following accidents (where project compliance cannot be demonstrated in court) have severe repercussions; senior company officers face jail sentences and companies pay substantial fines.

Industrial matters

The wider industrial environment can significantly impact on the project at large as trade unions and other representative bodies have to be considered as part of the process.

Furthermore, the regulatory framework usually prescribes consultation as a mandatory element. This traditionally results in the negotiation of acceptable outcomes. While it is common to negotiate or “cut deals”, often by way of trade-offs, this invariably disadvantages one party over another.

With extensive project experience in industrial environments, Caravel understands the intricacies of the consultative process as well as its pitfalls. We avoid ‘deals’ and do not seek compromises; instead we are consistently successful with our approach based on logic, science and engineering discipline.

By focusing on safety engineering principles, our process promotes safety decisions that will

- effectively resolve differences of opinion
- align stakeholders in a win-win scenario
- withstand scrutiny by unions
- stand up to scrutiny in court

About embedded security

When new safety device components are introduced to existing systems they typically represent an introduced security threat. In a rail network, for example, the introduction of data loggers and event recorders in trains adds a new dimension of complexity with regards to the treatment and security of the data.

The data and its capture, while often sensitive in nature, clearly has to withstand rigorous scrutiny and must be forensically defensible in a worst-case-scenario.

It is therefore not uncommon for Safety Critical Projects to contain one or more security orientated sub-projects which have to be treated accordingly. (Refer to Security Management Projects brochure).

Managing Business-as-Usual Operations

Fundamentally, cost-benefit analysis is used to identify the most cost-effective control for an unacceptable risk.

It is imperative for Safety Critical Projects to consider the impact they will have on the Business-as-Usual operations, its policies, processes, practices and procedures.

This aspect requires particular attention given that Safety Critical Projects usually operate within a distinct multi-organisational operational environment, comprising meshed layers of infrastructure component owners, operators and the like. Managing a systematic organisational response to transition is therefore significantly more complex and demands a well-structured approach with clearly defined responsibilities.

This is typically addressed with a committee-driven governance regime, underpinned by a charter as well as trans-organisational auditing and reporting capability so that the new policies, processes, practice and procedures can be effectively put in place.

The Case for Change

Projects that promise to deliver a safety improvement first have to establish the safety case outlining the parameters for change. This is normally delivered as part of the safety management plan and in addition to the identification of the required risk assessments.

Costs vs. benefits

The safety case puts costs, benefits, risks and residual risks under the spotlight, notwithstanding the delicate nature of quantifying the benefits of safety changes. It must be considered that the implied cost of averting a fatality inevitably becomes a controversial matter in the public domain.

As a result, the cost/benefit analysis has to establish a sensible framework that allows little opportunity for data to be misconstrued by sensationalist media; e.g. aspects of lost productivity. Given the political sensitivities surrounding safety improvements, an integrated communications plan is vital to manage the public perception and reputation of the project.

How much risk is acceptable?

The cost of safety improvements is clearly related to the reduction of risk. However, reducing the risk to zero would require enormous, and potentially infinite, resources; this begs the question of "how much is enough".

Improvements are therefore widely tested against the ALARP principle, according to which the residual risk should be "as low as reasonably practicable" (some jurisdictions use AFARP "as far as reasonably practicable").

It must be noted that the risk reduction of individual components applies only to the components in question and not the system as a whole. Thus the reduction of a derailment hazard in a rail network by applying any one control technique - whilst that control may well be ALARP - does not render the entire rail network risk ALARP to the derailment hazard. The reduction of a hazard through the application of any particular control technique may well mean that the particular control has reached a risk reduction to ALARP. However, this does not necessarily mean that the hazard has been fully treated and reached ALARP as additional controls may well be needed before this point is reached.

Safety Critical Projects are difficult environments from a project management point of view. A wide range of safety standards, methods, concepts and technical complexities demand a sound understanding of how they impact on the project.

Frequently confused concepts:

The **Safety management system** refers to the methods that address an organisation's approach to safety.

The **Safety system** comprises the controls that are used to ensure the safe operation of a system or equipment in service.

The Business of Safety Management

Guiding parameters

A number of accepted standards and methodologies are associated with safety risk assessments. Some common examples are:

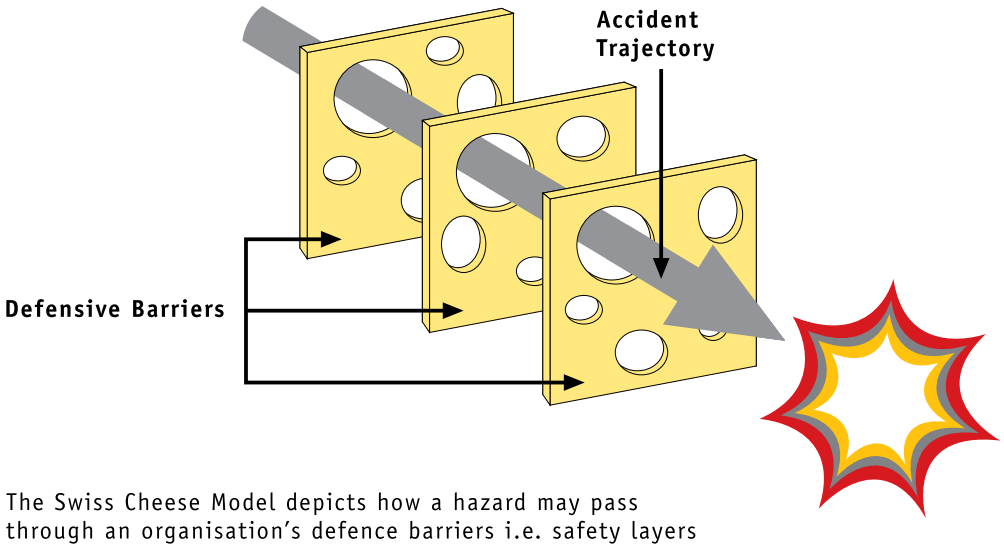
- AS/NZ 4360 General Risk Management Standard
- Industry specific standards e.g. AS/NZ4942 and EU 50126 (RAMS) for the rail industry
- Standards for electronic equipment such as AS/NZ 3932, IEC 61508 (SIL)
- AS/NZ 4801 OHS safety standards
- HAZOPS for manual process oriented safety system
- Fault- and Event Tree Analysis
- Threat barrier and Bow-Tie Diagrams

Concepts to consider when assessing risk

The ability to perform accurate risk assessments is vital for Safety Critical Projects. The assessment process has to consider the wider project context and aims to maintain it during the entire assessment period.

Throughout the process, Caravel adopts a life-cycle view of risks and addresses them during all work streams, from the initial analysis & design phase right through to support & maintenance.

In the field of occupational risk prevention, a number of models have been established. James Reason's Swiss Cheese Model assesses risk in context of safety layers and dimensions. It suggests four generic levels of failure (organisational influences, unsafe supervision, preconditions for unsafe acts, and the unsafe acts themselves) and models an organisation's defences against failure as a series of barriers, represented as slices of Swiss cheese. The holes represent individual weaknesses, which – when they momentarily align – allow a hazard (should it occur) to pass through the holes in all the barriers, leading to failure of the safety system as a whole.



The Swiss Cheese Model depicts how a hazard may pass through an organisation's defence barriers i.e. safety layers

Caravel's decomposition of safety layers

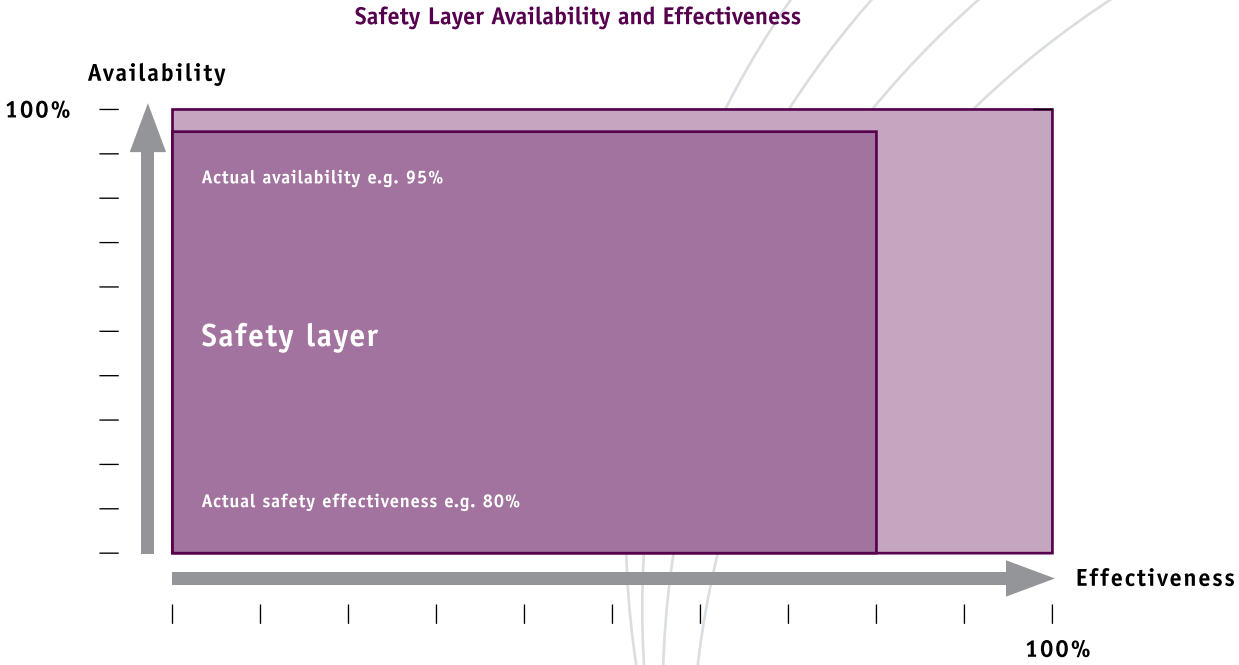
The Swiss Cheese Model affords 'structural insight' into risk layers, however fails to consider availability and effectiveness.

Caravel has further developed this model so that it also addresses the availability and effectiveness of the layers to perform. We have found that this approach affords a more accurate view of the actual risk on a practical level.

After all, when a defence layer is available 95% of the time, but with 60% effectiveness, its precise level of protection is only accurately reflected in Caravel's differentiated approach.

Safety layers

Safety systems typically feature a number of usually interrelated safety layers, designed to prevent or mitigate accidents. Possible threats and their respective safety layers are usually depicted in Bow-Tie Diagrams which graphically represent the various safety layers that prevent specific hazards and those that treat the potential consequences after the occurrence of the hazard.

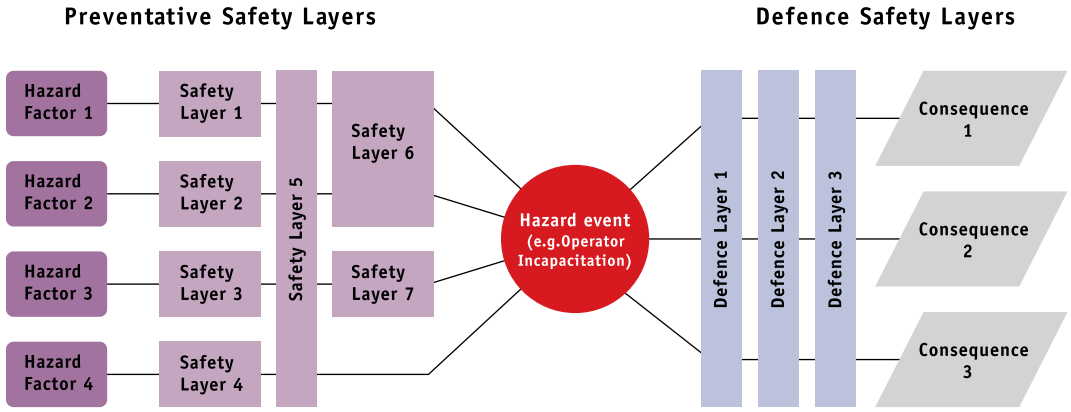


Preventative safety layers are often procedural in nature. A rail network, for instance, would prevent driver incapacitation through safety layers such as drug and alcohol compliance, a health and wellness programme, medical testing, fatigue management and the like.

Defence safety layers, on the other hand, mitigate the consequences of hazards and usually represent safety devices. A rail network, for instance, employs Train Stop Trips, to mitigate against derailment.

The introduction of a new safety device has to be carefully assessed in terms of its impact on existing safety layers. The assessment considers the availability and effectiveness of existing safety layers and adopts a strength & weaknesses matrix to demonstrate the contribution of the new safety device to the overall risk mitigation.

The relative merits and demerits of the safety case have to be weighed up against its impact on operational effectiveness. Similarly, the safety case needs to be viewed in context of the project delivery costs.



The Bow-Tie Diagram depicts the various safety layers

Modelling techniques

In addition to Bow-Tie Diagrams, risk may also be analysed using modeling techniques such as Fault Tree Analysis or Event Tree Analysis, keeping in mind the human tendency to arrive at satisfactory decisions despite uncertain data, by entangling the proverbial “statistics and damned lies”.

Frequency vs consequence:

Project managers often have to compare low-frequency high-consequence risks with high-frequency low-consequence risks. The compounding effect of the latter is often inadequately considered.

Similarly the Failure Modes, Effects and Criticality Analysis (FMECA) may be used in a variety of activities. The well established analysis identifies all possible failures within a system, the possible effects of these failures and any potential consequences. By ranking potential problems in terms of severity and criticality, the FMECA process can be used to identify and focus attention on areas of greatest concern.

Risk assessments also have to balance qualitative and quantitative models, and relative risks with absolute risks.

The human dimension

The recognition and study of human factors is important for Safety Critical Projects because they can cause serious human errors on the levels of cognitive decision making and physical behaviour. Cognitive ergonomics addresses matters related to operator distraction, fatigue as well as environmental aspects such as weather and other ambient factors. The field of physical ergonomics covers muscular skeletal impacts from within the operator’s environment.

The consideration of human factors also draws attention to the potential negative impact of safety systems on operators. This may result in fatigue, distraction etc. and bring its own set of risk factors. The choice of safety systems therefore requires careful balancing of all factors, ultimately erring in favour of “the greater good”.

Method limitations

The use of Fault Tree Analysis is limited to statistics that feature a two-state “pass or fail” outcome. Many human factor situations, by contrast, cannot be treated by such a two-state phenomenon due to the continuum of interrelated factors having dependent rather than independent variables.

Risk ownership

Risks are often shared by various parties. As outlined earlier, risk may be inherited or introduced through the supply chain. Once treated, the risks may be transferred as appropriate.

While the roles and responsibilities of parties must be clearly assigned, risks have to be addressed in such a manner that it ensures forensic defensibility in case of failure. After all, the legal implications can drastically affect individuals and organisations alike if the system is challenged and does not stand up to scrutiny in court.

Keeping the system going

Reliability and safety engineering is vital for Safety Critical Projects, allowing the system to perform its required function within the given parameters.

- Reliability engineering - identifies failures and defects of criticality
- Reliability centred maintenance - is an extension of reliability engineering and is usually concerned with the physical environment
- Safety engineering - takes a broad-brush approach and incorporates the physical and human environment

Risk management tools

Project management professionals can choose from an abundance of risk management tools. However, the tool itself is not an important differentiator, since the results are more dependent on the quality of the data used to populate the tool.

Situations often occur where available data is uncertain in terms of quality and quantity. Irrespective of the model that is being applied, this will inevitably produce uncertain solutions.

As a result, uncertainty is integral to safety engineering. The existence of uncertainty does not necessarily render solutions invalid - it simply results in a range of possible outcomes being established. It is vital that the uncertainty is acknowledged as such and addressed appropriately.

The Monte Carlo method may be used to simulate the safety system in order to demonstrate the effect of changes in input variables, where those variables occur in accordance with some form of random distribution curve e.g. normal distribution.

Delivering the solution

As a leader in complex multi-discipline projects, Caravel has completed a wide range of Safety Critical Projects and offers proven experience in this multi-faceted and highly complex environment.

Distinguishing types of risk

Project managers have to be mindful to clearly define, and differentiate between project risk and operational safety risk.

Project risks can affect schedule delays, budget consumption or the quality of deliverables. Operational safety risks, by contrast, arise from the use of machines (e.g. trains) or tools (e.g. mining equipment), and how their reliability affects public safety and the people who operate them.

Despite this distinction, it must be noted that project risks can influence operational safety risks in certain circumstances:

- While the project budget consumption per se has no knock-on effect, a project delay may well represent additional operational safety risks; the public and/or the operators may be exposed to additional risk by virtue of the missing safety capability, which would prevent safety incidents once deployed. There is no defence for unwarranted project delay.
- Project quality can have a similar effect on the availability and performance of the delivered safety critical capabilities.

The safety critical capabilities may comprise processes or technology, whereby the latter may be a mix of software and hardware operating in real time.

Given the nature of the environment e.g. processes reliant on technology-assisted decision-making within fractions of a second, a sense of mission criticality pervades the scene.

Transition and implementation

Safety Critical Projects will usually involve changes to an existing operating environment. This can result in the implementation of new business processes, new maintenance systems, new management reporting and new or upgraded ICT systems.

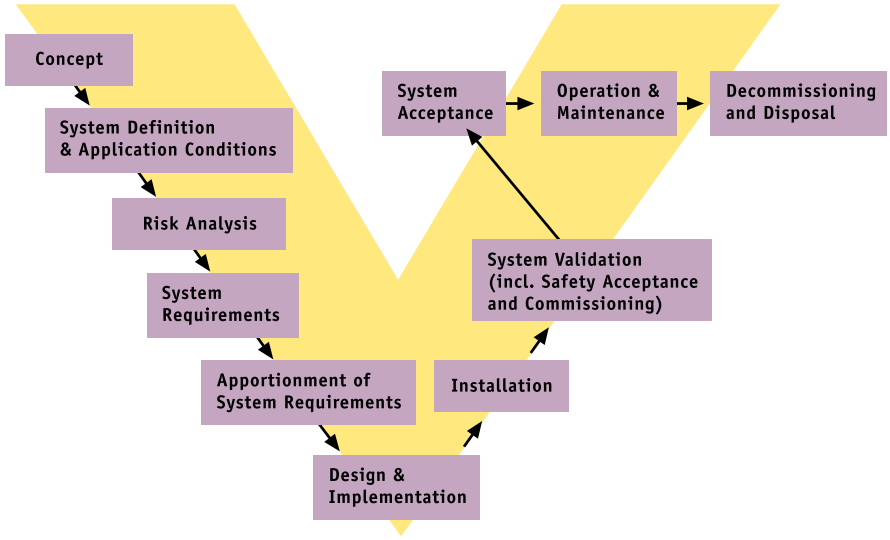
In order to ensure a successful system integration, the change management process therefore also has to address aspects such as operator training, maintenance crew training, spares and logistics as well as assessment of scheduling impacts and crew resource requirement impacts.

Making sure it works

The project assurance discipline of Independent Verification and Validation (IV & V) plays a pivotal role in confirming the basic underlying principles:

a) that we are building the right system (i.e. validation of what is produced against the objectives)

b) that we are building it right (i.e. verification of the steps)



The IV & V process of independent verification and validation usually adopts the "V-Diagram" (ref. EN 50126)

IV & V is executed across the entire project life cycle and adapts to the special characteristics of a project.

Processes include system integration elements and testing strategy for hardware, software, embedded systems and process elements prone to human error.

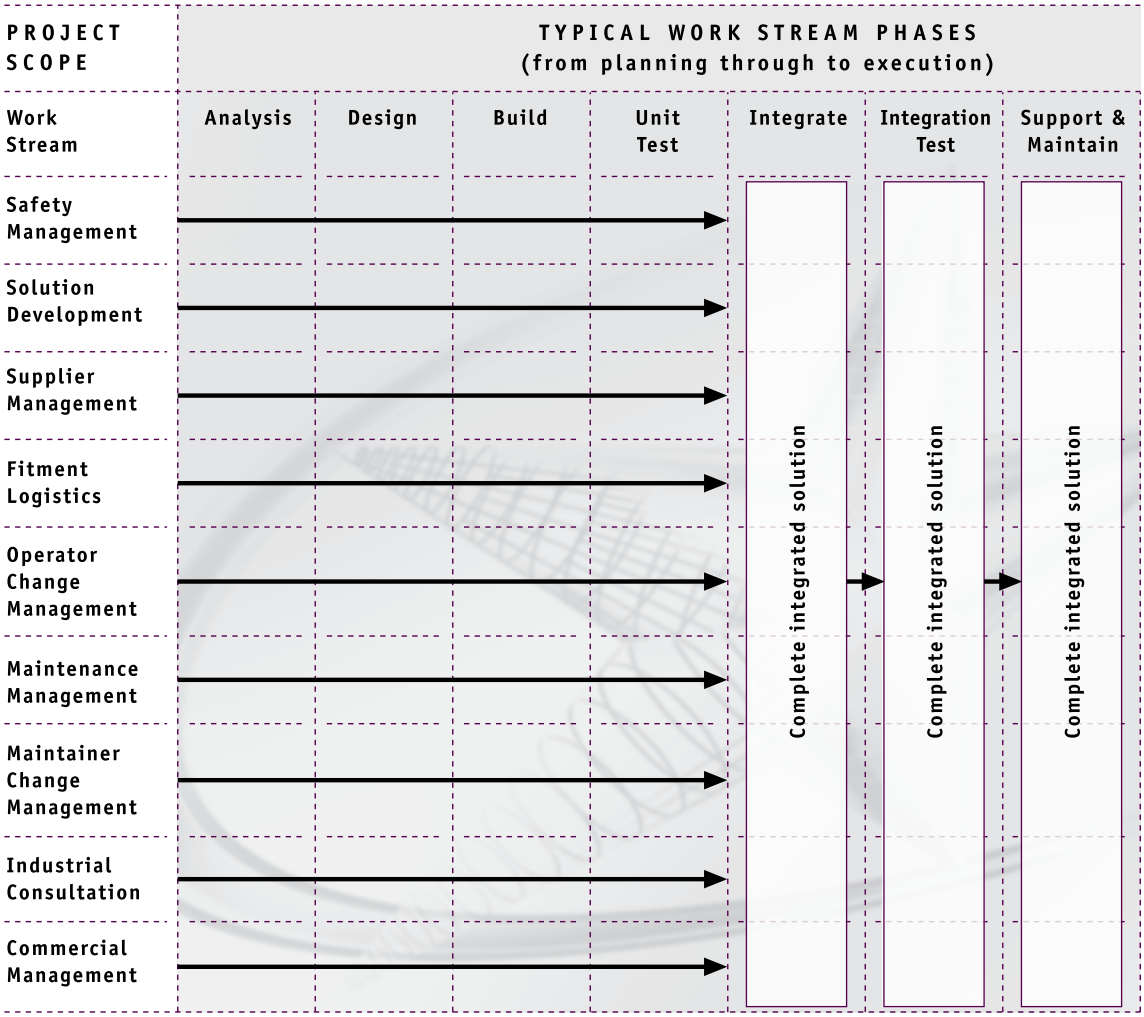
An independent verification and validation process is a fundamental requirement of Safety Critical Projects.

The IV & V process is vital for ensuring the correctness and quality of the system.

The Caravel methodology

Caravel responds to the multi-faceted project reality with a tailored approach that meets your specific Safety Critical Project needs:

THE CARAVEL METHODOLOGY



The work streams include:

- Project planning, monitoring and control and organisational interface management throughout the programme of works
- Safety engineering and compliance
- Solution specification and development
- Supplier solution procurement and management
- Fitment logistics management, testing and quality assurance
- Operational systems change management including business process development where required
- Maintenance management
- Organisation change management including training, recruitment etc. for both operators and maintainers
- Commissioning and transition support management

When you invite us to work on your Safety Critical Project, we will assess the needs of the project and the degree of skills and resources that are required to support the project. We may provide our detailed knowledge, work alongside your teams, transfer our skills and provide continuity after the project.

The initial assessment also addresses

- the requirements, scope and schedule of the project solution
- the project organisational interface management requirements
- the operational and organisational change management requirements for operations and maintenance

Please refer to Caravel's related brochures

- Change Implementation
- Strategic Management of Projects
- Business Process Innovation
- Enterprise Management Solutions
- Project Assurance
- Operational Management Centres
- Security Management Projects

Caravel
LEADING THE WAY IN PROJECTS

Caravel's range of project services

As a leader in projects, Caravel offers a range of specialised consultative and implementation services that span the entire life cycle of a project from inception, through implementation to final hand-over. Caravel adds value at every point along the way through project management services for:

Strategic Management of Projects
Core services include:
- Multi-project Management
- Organisational Resource Management
- Value Management
- Project Feasibility Studies
- Critical Chain Modelling
- Organisational Project Management Maturity Assessment

Project Assurance
Core services include:
- Project Governance
- Project Audits
- Project Health Checks
- Recovering Troubled Projects
- Project Risk Assessments
- Post-implementation Review
- Mentoring and Training

Project Planning and Execution
Change Implementation
Business Process Innovation
Business Partnering
Enterprise Management Solutions

Operational Management Centres
Core services include:
- Customer Contact Centres
- Service Management Centres
- Operational Control Centres
- Mission Critical Moves

Safety Critical Projects
Bid and Tender Management
Project Management Office (PMO)
Security Management Projects

Caravel can tailor a range of industry-specific services to suit the exact needs of your organisation.

Please refer to our website for your nearest Caravel office: www.caravelgroup.com