ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

Management of Change in an Ever-changing World

Keith Collyer[1] and Wendy Owen[2]

1. Independent Consultant: Systems Engineering, Requirements Management
2. Independent Consultant: Systems Safety and Assurance

Abstract

How do you manage change in a world of rapidly changing technology and ever-changing priorities? This paper discusses the roles of Management of Change (MoC) and Change Management (CM) in the context of systems being designed, built, and operated today. This is of particular concern where there are safety, security, or environmental issues. It is not that significant technological changes have not happened in previous decades, they have, but the nature, functionality and complexity of today's systems place a particular onus on traceability, auditability, and assurance, to ensure that these systems are safe and fit for purpose both for today's operating environments and for those of the future. MoC enables intelligent business decisions at every stage of the project, system, and safety lifecycles. Acknowledgement and integration of CM within companies, engineering teams, and projects is increasingly important for high-quality outputs and outcomes.

1 Introduction

The focus of this paper is on how managing change relates to the technical assurance of systems (Nagaveni 2024) (Bock and Feeney 2013) (Technosoft 2024). While some safety engineers may be familiar with the topics, we recognise that others are not. To that end, we will start with a discussion of why managing changes is important, and even essential in some cases, what you need to achieve through managing changes, when you need to manage changes, who should be involved, and an outline approach.

We will also discuss the relationship of change management to version control and configuration management, its significance in safety-critical applications, and why it is more of a necessity in today's world of rapidly changing technology.

Management of Change (MoC), alongside Change Management (CM), are as simple as they say — they define the management of change or changes. In this context, Management of Change is the high-level approach, that is, policy or strategy, while Change Management refers to the detailed process of managing changes.

It is worth noting that managing change also applies to users and other stakeholders in systems (HUCMI n.d.) — change of these types is often referred to as "transformation". The discussion in this paper pertains to the design of systems and related processes, rather than organisational changes, although many of the same principles apply. Within an engineering context, changes occur not only during the design phase but throughout the whole lifecycle, from concept to disposal.

Organisations that adopt a continuous improvement methodology can be a particular concern. There is an argument that something that keeps changing is harder to assure. If

© Keith Collyer and Wendy Owen 2025.

anything, this tells us that it is even more important to manage change in such an environment. Along with the approaches described in this paper, such organisations will probably use prototypes, pilot schemes, and phased deployment. While these are not strictly change management approaches, they limit the scope of harm if the change turns out to be inappropriate; consequently, they are outside the scope of this paper.

Refer to Appendix A for explanations of common terms used in this paper.

2 Why Manage Change?

Why should you manage change? Essentially, change management is an exercise in risk management. There are often risks associated with making changes — and, in some cases, with not making changes. The risks could be related to material, financial or operational continuity, or be associated with safety, environmental or security issues. MoC ensures that projects balance these risks against the benefits.

MoC is also about communication. It is important to communicate information about changes to relevant people and organisations. Different stakeholders will need different types, amounts, or levels of information about the change(s).

Finally, in many highly-regulated industries, appropriate conduct of MoC is a regulatory necessity, for example, the US Food and Drug Administration's Quality System Regulation, 21 CFR Part 820 (FDA 2024), applies to medical devices, and MoC within engineering safety management in the rail sector is integral to the Common Safety Method of (EU) No 402/2013 (ORR 2018), which is briefly discussed later in this paper.

3 What Needs to be Achieved? — Things to Consider

There can be many reasons for making a change. These can include changing functionality, changing performance, technology upgrades, replacing obsolete subsystems, replacing material, a change of operations, alterations to zone or location aspects (including externally), changes in the operational environment, fixing defects, improving systems, upgrades, or for regulatory or standards reasons. For example, a widget has a design life of ten years, and you want to replace it with one that has an improved design life of twenty years, and for use in a different country with a wider scope of ambient temperatures. An organisation may wish to use another version of a widget in a different sector which has more stringent requirements for safety; the widget then needs additional or modified design features.

Changes are often related to safety, performance, reliability, or availability targets, or other Key Performance Indicators (KPIs); for example, tightened safety targets, or related to improved performance, for example to increase plant throughput. Functional change and upgrades are also prevalent in industry.

Before making a change, a number of aspects need to be considered. These include:

- The reasons for and expected benefits of the change.
- The effects and risks of not making the change.
- The impact of the change:
    - On other artefacts or systems;

- On people, the environment, safety, or security;
- On stakeholders;
- On processes or operations; and/or
- On any other interfaces.

- The cost of the change itself, and
- Consequential costs of the change.

Changes need to be fully traceable or auditable. You need to record the reason for the change, when it happened, what changed, how it changed, and who was involved. In most cases, an appropriate authority, typically a Change Control Board or change management team (see below) needs to approve changes. In some organisations changes will be approved by other authorities, for example, the Design Authority, Safety Team, or Approval Panel — different organisations use different terms.

4 When Do You Need To Manage Change?

Change management is an overhead with a non-trivial cost. So, it makes sense to specify what sorts of changes that projects need to manage. Once anyone other than its creator is using any artefact as part of a working system or process, then the artefact needs to be under change management. Change management is also needed during the design or upgrade process as a project record and for technical audit purposes. If there are safety implications of the change, a formal process will be needed, and safety audits can be expected.

For sufficiently significant changes, definition and implementation of the change can be a project. You would therefore use Project Management (or even Programme Management) techniques to manage the change[1]. Does this mean that Change Management is not relevant to these significant changes? The answer is no, for two reasons. First, and most obviously, you apply Change Management within the project or programme. Second, the decision to go ahead with a project or programme should follow the same framework as any other change. This naturally raises the question of when you need to apply full Project or Programme Management. A full answer is outside the scope of this article and will vary between organisations, but things to consider include:

- The expected cost of the change
- The expected impact of the change
- The availability of resources

Some changes are not typically covered by change management procedures. For example, routine maintenance involving replacing one part with another because of wear does not usually involve change management, though this would usually be recorded. Similarly, logs and other contemporaneous records are additive, and are typically not under change control, except for hazard logs or registers as found in safety-related sectors — in this instance, it is not only the change itself that will be assessed for safety implications, but each entry in the hazard register demonstrably affected by the change will also itself be under change and version control.

[1] There is an argument that all projects are change projects. Discuss!

Questions to ask to decide whether a project needs to manage a change include:

- Do regulations state that you need to manage this type of change?
- Does any other system or process depend upon or interface with the system or process being changed?
- Is it a "Significant Change"?

The concept of "Significant Change" has a particular connotation in mainline railways ((EU) No 402/2013) (ORR 2018). When a proposed change has an impact on safety, the proposer must decide, by expert judgment, the "significance" of the change. The criteria include:

- The consequence of system failures: what are the most credible worst-case scenarios in the event of failure of the system, considering the existence of safety barriers?
- Any novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new for the organisation implementing the change.
- Complexity of the change; the more complex the change, the more significant it is.
- Monitoring: the ability (or inability) to monitor the implemented change throughout the system life cycle and the ability to make appropriate interventions.
- Reversibility: the capability (or inability) to revert the system to its state before the change.
- Additionality: assessment of the significance of the change, considering all recent safety-related modifications that at the time of earlier changes were not in themselves judged as significant (the cumulative effect).

The approach does not prescribe how to use the criteria, nor the priority or weighting given to any of them. The change proposer usually needs to undertake preliminary work to identify and understand the associated hazards before applying the "Significance Test" above. This also helps with selecting the most appropriate "Risk Acceptance Principle(s)". A simple matrix can help in forming a judgement of whether a proposed change is 'significant' (high uncertainty, high consequence) or 'non-significant' (low uncertainty, low consequence), or where the project needs to apply any other criteria to make a final decision. Thus, the implementation of any proposed "significant change" is effectively geared by the project's safety management system (SMS). For a significant change, the proposer must produce "*a written declaration that all identified hazards and associated risks are controlled to an acceptable level*". If a change is not considered significant, the proposer must be confident that risk is controlled to an acceptable level. The impact of change is likely to be different at different stages of the lifecycle; however, it should be recognised that later changes (post-build or installation) are typically the costliest.

The approach we describe here covers normal "sunny day" operations. In many industries, unplanned or unexpected events occur to which organisations must respond promptly by making changes. In such circumstances, the organisation must apply the normal Change Management approach retrospectively to the changes made. They must do this as soon as possible after the changes.

5 Who Needs to be Involved?

Consider the people who might be involved in any change. Who are they, and what is their role?

A change must have some actor who requests it. The Requestor may not have knowledge of how the system works, so may not be able to provide a specification or input on risks and costs of making the change, but they must provide a justification in terms of its benefits (or conversely of not conducting the change).

Most non-trivial changes will have a cost associated, so a budget holder needs to be involved and often makes the final decision on whether to go ahead with the change. However, in some cases, this final decision should also involve a safety or security manager, and in many industries, will involve a regulator.

In most organisations there will be some form of Change Control Board (CCB) and, although the name will vary, the intent and function are the same, that is to act as the focal point for all change requests and to have sufficient knowledge to be able to decide whether a change is necessary or worthwhile. Different people do this in different organisations. In some cases, this role is assigned to an individual, often the engineering manager or project engineer, or (for larger projects) a dedicated change manager, but it is usually better to have a team. The typical membership of such a team includes:

- A designated CCB Manager;
- Representatives of the Quality Assurance organisation;
- Safety, Security, or environmental engineers, as relevant;
- Specialist engineers, including those who will be involved with the implementation of the change and those responsible for systems that interact with the system to be changed;
- User experience and user interface experts;
- Stakeholders, including in some cases the Owner of the asset, the Design Authority, other Technical Authorities, plus (externally) Approval Bodies and industry regulators (noting that external stakeholders do not normally sit on a CCB, but the CCB may liaise with them); and
- Other Subject Matter Experts (SMEs), as needed.

The CCB needs to consider the needs of other stakeholders, including the owners and operators of related systems, users, and potential regulatory impact. Last, but not least, those responsible for implementing the change must be involved. They will handle determining costs and timescales for making the proposed change.

6 When and Where?

Here we consider a few “whens and wheres” — when in the lifecycle, and where in terms of location.

When in the lifecycle is the change happening?

- At concept stage? During “optioneering”?
- During design?
- During installation, construction, or build?
- During operation?
- During maintenance or a shutdown?
- For advance planning or futureproofing
- For decommissioning, dismantling, or disposal?

The lifecycle phase where the change is happening often requires different processes and people. Continuity of the change management process throughout the rest of the lifecycle is particularly important for changes or modifications with safety implications.

Where is the change happening in terms of location?

- In a manufacturing facility?
- In a design office?
- On or off-site?
    - If on-site, in which zone — do adjacent zones need to know?

A change, if not effectively managed, could set off a "domino effect" if it goes wrong, or if external interfaces have not been sufficiently considered.

7 Change Management Plan and Change Register

The Change Management Plan (CMP) defines the policies for the Management of Change in a project. It is a key document in any engineering project, and this should be adapted and kept live throughout the project lifecycle, alongside a Change Register. It should link directly with other project engineering plans (particularly with safety, security, and environmental management plans, as relevant). The Systems Engineering Management Plan, "SEMP", and any Technical Assurance Plans, such as the Systems Safety Management Plan, should cross-reference the CMP.

Organisations typically have a higher-level policy document that applies across all projects and from which the projects derive the individual Change Management Plans for their projects.

The individual changes for a project, regardless of their status (Rejected, Approved, Implemented, …) must be recorded in a Change Register that holds the what, why, where, who, when and how of changes for a project. Threat and Hazard Registers and Logs, where relevant, should cross-reference relevant change register entries, to enable full traceability and assurance justifications.

8 How to Manage Change — An Outline Change Management Process

8.1 Procedure

Change Management defines how to manage changes day-to-day. An organisation typically has a Standard Operating Procedure (SOP) defining how it approaches Change Management. Depending on the nature of the work, departments within an organisation or individual projects may amend the SOP to suit their purposes. Such amendments will generally be agreed upon by the owner of the organisation's SOP and are intended to allow flexibility for specific different uses than the organisation's SOP. They must not allow different procedures to be used for each change.

Figure 1, overleaf, shows an example process for Change Management that we further describe in this section.

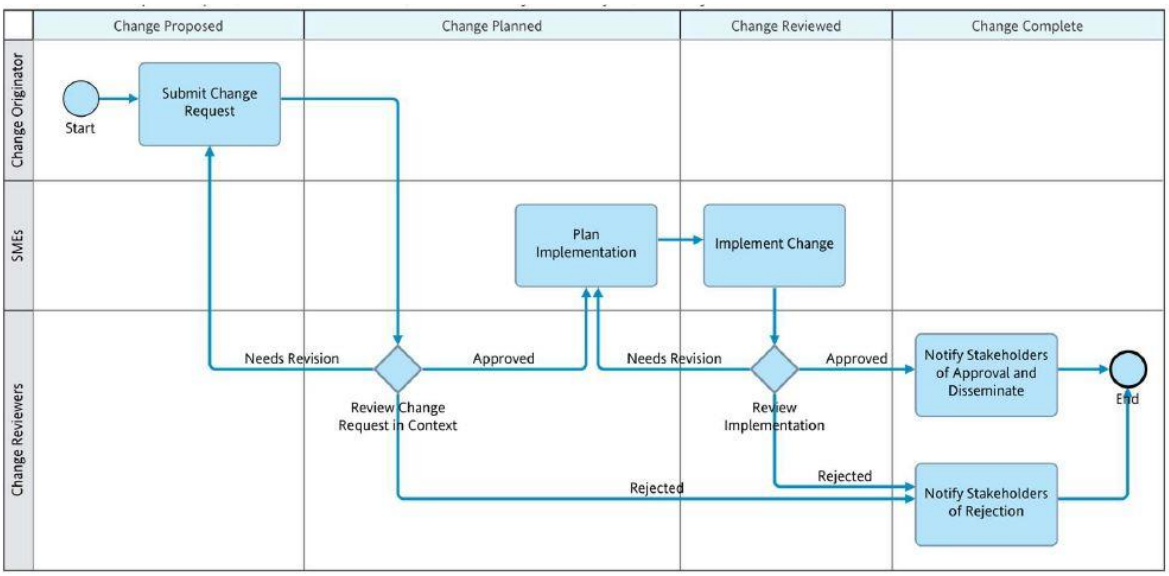


Figure 1 ~ Generic Change Management Framework

Note that any suitably qualified person or body can reject a change at any stage, not just at the formal reviews. We do not show this on the diagram for the sake of clarity.

8.2 Roles

The example process in Figure 1 uses the following roles:

- Change Requestor: The person or organisation that initiates the change request.
- SME(s): The Subject Matter Experts involved in planning and implementing the change.
- Change Reviewer(s): Typically, also SMEs, with the specific roles of reviewing change requests and their implementation.

8.3 Submit Change Request

The Change Process formally starts with the submission of a Change Request. However, several actions must be carried out before this can happen.

Someone must identify the potential need for a change. Typical prompts for this include:

- Identifying a pattern of failure
- Identifying a new, better, or different result or product
- Identifying a better way of producing a result or product
- A change in the operating environment, or a change in external processes

Note that this identification focuses on the outcome of the change, not on how it should be implemented (though suggestions as to this are usually welcome). In many cases, the identifier of the change must do at least an initial impact analysis, or assessment of the safety (etc.) implications.

Typically, for safety-critical or high-risk changes, there will be a peer review, for example, an internal design review process, before formally submitting a Change Proposal.

Who can identify a change? In principle, anyone with any knowledge of the system concerned. In practice, this is limited to stakeholders in the system, but can include

indirect stakeholders who may not come into direct contact with the system but can be affected by it. For example, people with property adjoining a railway line, or the public need to cross the line at a level crossing, bridge, or subway.

Once a potential change has been identified it must be formally proposed to progress. Typically, this means completing a Change Proposal form. Generally, completing this form will involve other actors than the original identifier providing the needed information.

Typical information requested at this stage includes:

- Proposer
- Rationale for the change, including benefits and risks if not done
- Identification of the actors who will own the change (in the sense of progressing it) and who will be responsible for delivering the change. These could be the same or different.
- Nature of the change — outline of what must be modified to deliver the change.
- Anticipated cost of making the change
- Risks of making the change
- Any identified impact on other parts of the current system, external systems, or interfaces
- Importance of the change (priority and urgency, including associated timescales and deadlines)

8.4 Change Reviewed [and approved for go-ahead]

Before implementing a change, the appropriate authority must review it. Typically, this will be the Change Control Board, but may also take place in other settings, for example, a Design Review. The review must cover:

- Purpose of the change
- Impact of the change
- Consequences of the change
- Conformity with requirements
- Mitigation of any adverse effects
- Cost of making and implementing the change (in making this assessment, some idea of the implementation is necessary)
- Consistency with organisational strategy
- Regulatory implications
    - In some cases, regulators will need to review changes independently.
- Assessment of safety etc implications

The CCB has three options:

- Approve the change.
- Request revisions
- Outright rejection

If the CCB does not approve a change, it must formally record the rationale behind the rejection. At this point, the project may wish to return to earlier steps to look at further optioneering, or the design features, or other influencing factors. If the CCB requests revisions, in some cases the change may go ahead under advisement, but not be installed,

subject to the risk that it may be rejected later. In some cases, if the changes meet repetitive refusal the project may choose not to continue. This emphasises the need for MoC from an early stage in a project.

For safety-critical applications, the CCB usually includes a Safety Manager or Safety Design Authority (or similarly titled), as well as representation from Human Factors and Occupational Health and Safety. For this stage, an Independent Safety Assessor (ISA) or Independent Competent Person (ICP), for example as defined by the IET (2024), is usually involved in reviews of any safety-critical change.

8.5 Plan Implementation

If the CCB approves the change, it can be implemented. Decide whether and when this change should be scheduled, considering other related candidates, and the overall strategy.

Create a Plan that lists all tasks needed to implement this Change. This plan assigns individuals to tasks.

At this point, the team has assigned resources and intended timing to the Change.

Note that, if artefacts are sent back for revision after a later review, the implementation might need replanning.

8.6 Implement Change

The proposed change must be implemented exactly as expected or proposed, as not doing so could invalidate safety arguments, for example.

After the change has been implemented, but before installation and final sign-off, it is assessed and verified as being correct. This is typically done by the implementors. Independent verifiers verify and, if appropriate, formally approve the change.

For safety-critical applications, suitably qualified and experienced personnel (SQEP) should conduct the safety verification process, as this forms part of the safety lifecycle.

8.7 Review Implementation

The final approval for the change is conducted by the appropriate authorities — CCB, approval committees, regulators. Depending on the nature of the change and the system to which it is applied, this could be based on the results of the change assessment, or it could be done in-service. In the latter case, we recommend a way of falling back to the pre-change state exists.

For a safety-critical application, a Safety Manager or Safety Design Authority, Panel or Committee is usually involved in final internal signoffs. An ISA or ICP is also usually involved. External regulators may also need to assess and approve the change where there are implications for human safety or environmental safety.

8.8 Notify Stakeholders

Regardless of the decisions of the CCB and other authorities, it is important to notify relevant stakeholders and (for safety applications) the dutyholders, if they are not already engaged in the process. In the case of a rejection, these will include any stakeholders and dutyholders who have been involved in the change process. In the case of Approval, this

will include all those stakeholders plus any others who will be affected by the change but have not yet been involved.

8.9 Post-Implementation Monitoring & Review

Post-implementation, the change — or the impact of the change — should be monitored, to ensure that the modified system is 'performing as expected'. This is typically not considered part of the change management process itself, but many organisations, particularly in safety-critical domains, will implement intensive monitoring for a period after a change has been made.

For safety-critical applications, monitoring is an ongoing requirement to ensure that the system remains safe for use. The monitoring processes or systems may themselves need changing to be able to take account of the modifications.

9 Relationship to Version and Variant Control

Change Management (outside of software development) is primarily about individual artefacts. However, organisations need to consider the knock-on, or ripple, effects of changes to other parts of a system than the one directly being changed. Does it need more space or weigh more, and what impact does this have on other components? Does it need different interfaces, more power, etc.?

Within software development, change management is part of version control. In practice, this does not cause confusion, due to how software change control and version control work together.

Versions are generally associated only with artefacts that are, in some sense, in use or available for use. For example, when a new design for a specific artefact is issued, that will be an updated version of the design, because it is intended that further work based on the design will be done to create an updated version of the artefact itself. Of course, the design is itself an artefact. Each version of an artefact is assigned a unique version identifier. While versions typically progress chronologically, with an updated version supplanting an earlier version, multiple versions of an artefact can exist simultaneously. This is particularly the case where multiple instances of an artefact are in use at the same time — different instances can be, and often are, of different versions.

The Version Control process often incorporates auditability of changes. This is particularly important where the change has actual or potential safety implications. Variants and versions require particular care in a rapidly changing environment, and for market acceptance.

The distinction between a version and a variant is subtle and the two terms are often used interchangeably. The essence of the distinction is that different versions are typically interchangeable (at least, later versions can replace earlier ones), while different variants may perform the same functions but could have significant differences in their implementation.

For example, an object scanner for an airport runway compared to a variant of it for use at a railway level crossing, or the same scanner used for several different types of level crossing. However, at some stage, the 'baseline' scanner may get updated, creating an updated version of it, which then needs to be updated and rolled out across all its applications. Similarly, for Microsoft Office, there are Windows, macOS, and browser-

based variants. Each new release of each variant of Office is a new version with a distinct Version ID (and Microsoft will have several internal versions or builds before issuing a release). Other examples include hatchback and saloon variants of a car, or components that perform the same function and are internally the same but have different interfaces.

10 Relationship to Configuration Management

In most systems, it is necessary to know not just which artefacts are part of the system, but specifically which versions of each artefact, and how all the artefacts connect. This is the job of configuration management.

Configuration management is particularly important when there are multiple instances of a specific type of artefact, each made up of other artefacts, and where each could have different versions of some of those artefacts.

You cannot manage configurations without managing versions, and you cannot manage versions without managing change.

In some circumstances, maintenance changes are also covered by configuration management, for example, where it is necessary to identify a specific part by serial number.

Configuration management is good practice in systems engineering; any systems with safety implications should be subject to safety audits, and these should be able to easily identify which configuration and version are present at that stage of the project. It is particularly relevant to systems which form a system of systems.

11 Looking at Today's World and the Future of CM and MoC

In a world of rapidly changing technology, increasing cyber threats and adapting systems for climate change, it is becoming increasingly important for engineers to work with upgrades and manage the changes at all levels. MoC and CM are important for security (including cybersecurity), safety, and environmental reasons, as — done well — they capture the *raison(s) d'être* of the change(s). This can then feed into the safety, security, and environmental cases.

However, in such a world and with an increasing number of KPIs linked to external factors, such as societal or environmental changes, assessments and documentation can also quickly become out of date. It is thus essential to link the safety case version to the system version, or any arguments in the safety case can quickly become redundant and the safety case invalidated (the same applies to security and environmental cases).

Legacy systems being upgraded with modern technology or adapted for reasons of climate change are a particular example where many changes could be implemented and require significant assessment and documentation updates.

Within the MoC process, give consideration to the delivery of outcomes or overall goals rather than specific outputs. In this manner, both MoC and CM can better support longer-term business goals and KPIs in an ever-changing world. In today's world, it is thus also important to manage change to enable outcomes, not only outputs.

At the time of writing, developments in digital twins, cybersecurity, autonomous systems, and artificial intelligence are all "in the picture". Technical publications, as well as the news more generally, are now full of such stories. How safe will all these new systems be without full lifecycle traceability of their origins and builds, and a sufficient safety justification? How will they be accepted for use, i.e. by technical authorities, approval bodies and/or regulators, without good records as to how they came into being? A contemporary example is the current concern over AI safety, and the recent international report on the subject (DSIT 2024).

Acknowledgements

Thank you to the organisers for taking this paper as the basis of a workshop at the 2025 Safety-critical Systems Symposium, SSS'25.

References

Bock C., and Feeney A. B. (2013). *Engineering Change Management Concepts for Systems Modeling*. Report NISTIR 7922, National Institute of Science and Technology. http://dx.doi.org/10.6028/NIST.IR.7922. Accessed 9th September 2024.

DSIT. (2024). *International scientific report on the safety of advanced AI: interim report*. Department for Science, Innovation and Technology, DSIT 2024/009, 17th May 2024. https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai/international-scientific-report-on-the-safety-of-advanced-ai-interim-report. Accessed 9th September 2024.

(EU) No 402/2013. (2013). *Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment.* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0402. Accessed 9th September 2024.

FDA. (2024) *Medical Devices — Quality System Regulation*. 21 CFR Part 820. The United States Food and Drug Administration. https://www.ecfr.gov/current/title-21/part-820. Accessed 9th September 2024

HUCMI. (n.d.). Human Change Management Institute website: https://hucmi.com. Accessed 9th September 2024.

IET. (2024). *Independent Safety Assurance Factfiles*. The Institution of Engineering and Technology. https://www.theiet.org/impact-society/factfiles/isa-factfiles. Accessed 9th September 2024.

Nagaveni S. (2024). *Effective Engineering Change Management Strategies*. Techno-PM, 3rd June 2024. https://www.techno-pm.com/blogs/change-management/engineering-change-management. Accessed 9th September 2024.

ORR. (2018). *Common Safety Method for Risk Evaluation and Assessment — Guidance on the application of Commission Regulation (EU) 402/2013*. Office of Rail and Road. https://www.orr.gov.uk/sites/default/files/om/common-safety-method-guidance.pdf. Accessed 9th September 2024.

Technosoft. (2024). Best Practices for Engineering Change Management. Technosoft Engineering Projects Ltd., 22nd January 2024. https://technosofteng.com/guide-to-engineering-change-management/. Accessed 9th September 2024.

Appendix A. Terms and Explanations

Note: This table of terms is not comprehensive or definitive; we present it for guidance. Different organisations may use different terminology and definitions.

Term	Alternates and Abbreviations	Explanation
Approver	Design Authority, Safety Authority, etc.	Actor responsible for an internal signoff. In some situations, it could also involve external signoff (see ISA).
Artefact	Work product, Component, Part, Item, Element, System, Sub-system, System of Systems	Any item, physical or digital. Typically used for those that are in use or are planned for use.
Auditable	Traceable	A view that the origins of the artefacts can be adequately traced, through a series of changes that have been recorded in the change register.
Baseline	Core, Original	A Baseline is a Version, Variant, or Configuration, typically created when approval or acceptance is sought or has been received. Baselines are often used as points to which one can revert.
Change	Modification, Alteration	Changes may be physical, functional, material, or geographical.
Change Control Board	CCB	A team or group specifically responsible for monitoring and approving changes.
Change Management	CM	The practical implementation, process and tasks associated with generating an auditable and verifiable trail of the changes to an artefact or process
Change Management Plan	CMP, Change Process	A technical plan, often supporting other engineering management plans, which holds the overall approach to MoC and the details of the CM process. On larger projects, the two may be separate documents, or the MoC strategy may be part of a wider engineering management plan.
Change Proposal	Change Request	A formal document describing what the planned change is, who will be responsible for it, how it will be done, when it is expected to be done, and how much it is expected to cost.

Term	Alternates and Abbreviations	Explanation
Change Register	Modifications Register, Change Log	A formal register of changes that have occurred. Often stored in a database.
Configuration	Combination, Architecture, Structure	A defined combination of artefacts, each with a specific version, arranged in a defined manner. Typically, all artefacts of the same type will be of the same version, though this is not necessarily the case.
Configuration Management	Configuration Control	Management and recording of system changes in a step fashion, during the overall change.
Dutyholder	Responsible Person	An organisation, or a team or person within an organisation, who holds the (legal) responsibility for safety.
ISA	Independent Safety Assessor (or Auditor), Independent Competent Person (ICP)	A third party (separate from the project and companies involved in the project) who takes an objective view of a project, to provide independent assurance, verification, or authorisation that the artefact is safe for use and operation.
KPI	Key Performance Indicator	KPIs evaluate the success of an organisation, activity, or system. KPIs provide a focus for strategic, operational, and continuous improvement. They create an analytical basis for decision-making.
Management of Change	MoC	The top or high-level view, policy or strategy associated with changes that take place [on a project].
Quality Assurance	QA	Quality may apply to the artefact, process, people, or all three.
Regulator	Authority	A third-party body that approves the system for being safe and fit for purpose before operation or being placed back into service.
Requestor	Actor, Initiator	The team or individual proposing the change.
Risk	Technical Risk, Project Risk, Safety Risk	A combination of consequence and likelihood. May be qualitative, semi-quantitative or fully quantitative.

Term	Alternates and Abbreviations	Explanation
Safety Management System	SMS	The framework within an organisation or project within which safety and hazard management is managed. It provides a pro-active and systematic approach to managing, identifying, assessing, addressing, controlling and minimising safety risks. Although with a technical focus, it can also often include aspects of leadership, culture and responsibility. Risk management is a fundamental part of an SMS.
Stakeholder	End User, Interested Party	Any person, body, or organisation that has an interest in a system. Note that they may not necessarily have direct involvement in the working of the system, for example, residents of property adjoining a railway line.
Suitably Qualified and Experienced Person	SQEP	A suitably qualified and experienced engineer in systems or engineering safety and associated disciplines.
Subject Matter Expert	SME	An acknowledged expert in a specific field.
System	System of Systems	In this context, the scope of artefacts that you need to consider when making a change.
Traceable	Auditable, Trackable	The ability to identify the source and dependent material for an artefact.
Variant	Issue, Revision, Rev., Mod., Release	A distinct definition or implementation of a specific artefact representing differences in properties. Typical examples include saloon or hatchback variants of a car model, or components that are identical other than interfaces.
Version	Issue, Revision, Rev., Mod., Release	A particular form of an artefact that differs in certain respects from an earlier form or other forms of the same type of artefact. Versions typically represent chronological development. Different versions have different version identifiers.
Version and Variant Control	Revision control, Release control	The process of ensuring that versions (and variants) are appropriately managed and identified.

This collation page left blank intentionally.