ALTEN TECHNOLOGY

MODEL-BASED SYSTEMS ENGINEERING: AN ENABLER FOR REGULATORY COMPLIANCE

by Jared Dean, Codey Henderson, and John Gardner
Updated 21 March 2024

10875 N Dover St #500
Westminster, CO 80021

ALTEN

THE PROBLEM

When working on new products, or even enhancements to existing products, developers can lose sight of the end application and user experience. This is particularly concerning when developing products on a schedule and budget and where investment has already been made. Without model-based systems engineering (MBSE), design teams will find it difficult to define concretely the performance and regulatory requirements of the devices they develop, thus adding additional risk and uncertainty to the effort.

EXECUTIVE SUMMARY

Whether working in the US Food and Drug Administration (FDA)-regulated medical field or explosive industrial environments, using MBSE provides the confidence, traceability, and structure to meet regulatory requirements. We propose the methodology to optimize schedule predictability and development of the most appropriate products. In this paper, we briefly describe the systems engineering process being employed as well as two case studies that make the case for MBSE as a key enabler of efficient design to complex regulations.

INTRODUCTION

Use of MBSE tools and systems engineering best practices provides the confidence, traceability, and structure to efficiently develop products in regulated environments. This has been found true whether working in the FDA-regulated medical field or in explosive industrial environments. When requirements, functional definitions, architecture, and verification activities are captured in an integrated database model, the burden of proving compliance to an auditor is significantly simplified. In this paper, we briefly describe the systems engineering process being employed and explore two case studies that make the case for MBSE as a key factor in implementing efficient design under complex regulations.

The first case study describes Client A, who designed a medical device compliant with FDA requirements while using less than 10 percent of the project man hours on systems engineering and regulatory compliance activities. We demonstrate that the output of the systems engineer meets most of the FDA design control requirements. Moreover, because of the systems engineering efforts, the involvement of the quality and regulatory roles on the design phase was minimized to the final approval of the generated documents.

The second case study describes the use of the MBSE database as a requirements management tool for the analysis of complex standards. Client B works in the heavily regulated explosive atmospheres industry and used MBSE to wade through complex, parallel requirements to establish a clear verification roadmap for future products. This effort has reduced the time required to develop a new product by more than three months and has given the design team the confidence to innovate while minimizing the cost and schedule impact of third-party certification.

BACKGROUND

ALTEN Technology is an engineering services company that provides innovative solutions for engineering, IT, and product development projects across the product life cycle. We provide support across industries including aerospace, defense, automotive (including commercial vehicles), medtech, life science, rail, energy and environment, robotics, unmanned systems, and more.

Because ALTEN Technology works across a wide variety of industries, we have developed the systems engineering process with an emphasis on flexibility so that minimal changes are required for the baseline tools, regardless of the target industry. Clients in this business space often question the value of activities which fall outside the realm of traditional engineering efforts (i.e., design, CAD, and analysis). By necessity, we have honed the systems engineering process presented in this paper to create scalable tools to match the level of effort and realize the highest return on investment.

THE APPROACH

INTEGRATION OF THE PROJECT MANAGER AND SYSTEMS ENGINEER

One theme we reference throughout this paper is the difference between a project manager and a systems engineer. For the purpose of this paper, a project manager (PM) is the individual who manages the project deliverables including scope, cost, and schedule. In addition, the PM is often responsible for project risk management, resource allocation, and interaction with the client. By contrast, a systems engineer (SE) manages the system definition, technical risk, and implementation of the technical design. In general terms, the PM manages the project while the SE manages the product design.

Several sources specify and separate the domains of the PM from that of the SE (Kasse 2003; Haskins 2010); one of the clearer delineations is provided by the NASA Project Management and Systems Engineering Framework (NASA 2011). Our experience has been that small to medium projects are overburdened by the use of separate resources for project management and systems engineering tasks. Alternatively, a combined resource that embodies both the project management and systems engineering tasks adds significant value through synergy and results in a lower overall project cost. This bias toward a combined project manager–systems engineer role is assumed throughout the paper and supported by the discussion on regulatory compliance provided below.

PROPOSED SYSTEMS ENGINEERING PROCESS

The ability for the systems engineering process to be scaled is key to a successful implementation of systems engineering for small to medium projects. We developed the process in Figure 1 to accommodate the wide variety of industries and sizes of projects seen in the engineering services environment. One of the primary goals of this process is to allow flexibility by dictating high-level activities but not low-level processes. The SE process is integrated into each of the product development phases. In requirements and systems architecture, the SE works on product definition, including activities of hazard analysis, system requirements, and architecture. During concept design, the SE is engaged to ensure the product meets the system definition. During development, the SE works with the other technical resources to perform failure modes analysis and acts as a compliance check during the design review process. The SE is responsible for the integration effort and verification of subsystems and interfaces.

Although none of the activities shown in Figure 1 are new or novel, several elements have been tailored or added to the process. The first item of note is the integration of human factors, industrial design, and use case definition (functional flow) into the very early stages of the requirements gathering and architecture definition process. We have found that early engagement with industrial design leads to more innovative designs faster, as opposed to waiting until the concept design stage. Similarly, involvement of fabrication, assembly, inspection, and test (FAIT) representatives in the initial architecture discussion is critical to project success. The FAIT representatives are continually engaged throughout the process from early architecture brainstorming to production release; their addition minimizes downstream manufacturability changes. This continuous involvement helps capture manufacturing issues early, typically achieves cost of goods sold savings, and secures buy-in from a key group of stakeholders. The goal is to synchronize and integrate the design transfer process (production) with the design process for seamless handoff at the end of the project.

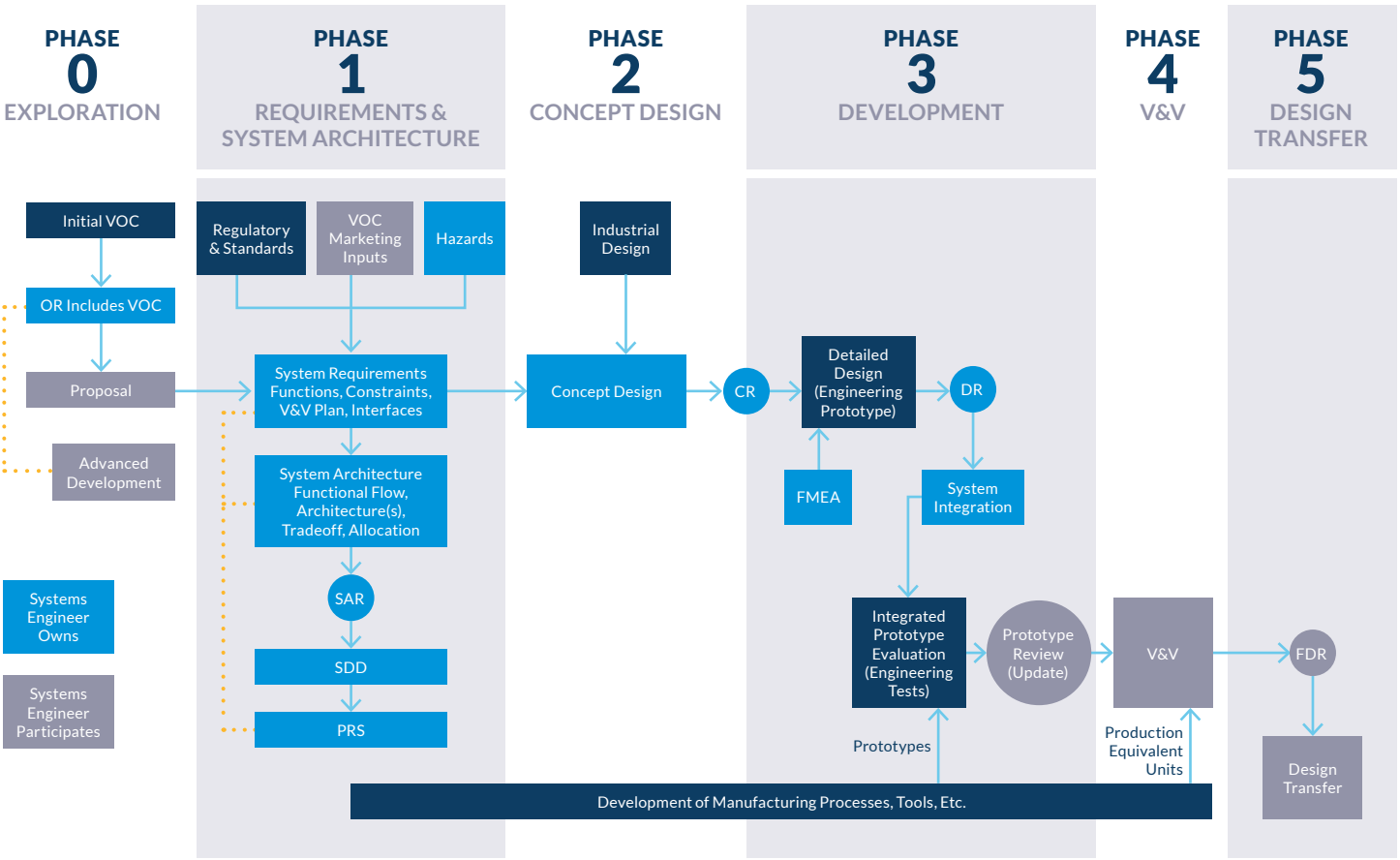
Another key element of the process is the use of a risk-driven prototyping strategy. Prototypes (also called mockups or engineering prototypes) are created throughout the design process for early-, mid-, and end-game verification and validation of the design. These prototypes are planned as part of the risk mitigation activity and their testing is tied to the verification and validation requirements. If there are significant technical risks, it is best to build some form of prototype to address them. If a verification requirement looks difficult to achieve, then a prototype should be created as early as possible for the specific purpose of that requirement. One example of a risk-driven prototype would be a foam mockup to validate a soft requirement such as “the product should be ergonomic.” Using the foam mockup early in the project to gain agreement on what constitutes “ergonomic” avoids significant design modifications later. These engineering prototypes are created as early as the system architecture phase and continued through to

the final, fully functional prototype validation activities. On projects with a high technical risk (low technology readiness level) the "prototype early" belief is pushed further, and an advanced development stage is added prior to the requirements definition to increase the technology readiness level (TRL) of the proposed system.

The following case studies used the process detailed in Figure 1, and one individual in the role of a PM–SE, in combination with an MBSE tool like Cameo. ALTEN Technology typically uses MBSE tools on large projects and projects that involve a regulated environment. For smaller projects in unregulated environments, the level of effort and documentation applied to these activities is only as large as is needed. Details on this scalable approach for non-regulated, small- to medium-sized projects can be found in Kolozs et al. (2011).

FIGURE 1. THE PROPOSED SYSTEMS ENGINEERING PROCESS

The systems engineering process offers deeper insight into procedural components. All members of the team come to an agreement on the activities occurring in each phase.



THE CASE OF CLIENT "A"

Client A specializes in the periodontal care market, making products for use by both dental professionals and consumers. ALTEN Technology was engaged by the client to redesign an existing product for increased functionality as well as system-cost reduction. We used MBSE-enabled systems engineering on this project because of the FDA-regulated environment, although the project is considered medium-sized (approximately sixty man-weeks).

The periodontal device is categorized as a Class I medical device, which requires that we apply FDA design controls (FDA 2010). An FDA investigator would examine the design history file (DHF) on a Class I device in the event of an audit and expect to see similar documentation to that contained in a Class II DHF.

The FDA details good manufacturing practice for medical devices in Title 21, Part 820 of the Code of Federal Regulations (CFR). While Part 820 has many sections that address quality system requirements, purchasing, and other enterprise-level concerns, Subpart C covers the requirements for design controls during product development (FDA 2010) that are the focus of this paper. The list of required design controls is surprisingly concise, requiring only that design and development must be planned, design inputs tracked, design outputs clearly defined and quantified, and the design reviewed. In addition, Subpart C requires specific planning and documentation of verification, validation, design transfer, and changes. Table 1 shows a listing of the FDA-required design controls. Importantly, the FDA mandates that the listed design controls must exist and be maintained, but not how they are to be created or maintained. This flexibility in the CFR leaves the door open for the use of standard systems engineering outputs to meet the requirement.

Table 1 shows how the bulk of the FDA-required design controls are satisfied by the output of the SE. The far-left column contains the FDA-required design control areas, the center column lists the proposed documents and deliverables that meet those design control requirements, and the far-right column lists the proposed owner of those documents. Any documents which are not the responsibility of the SE are primarily controlled by the PM or are direct outputs of engineering required for any design effort.

Because of the overlap of the responsibilities of the PM and the SE in regulated environments, it makes sense to have one person play both roles when possible. In the case of Client A, the PM and SE roles were filled by one person. In addition to aiding with regulatory compliance, the combination of the two roles typically leads to a more cohesive combination of technical and business roadmaps and risk management activities. If the size of the project requires that the roles be split between two individuals, it is extremely helpful if they are each qualified for either role or have strong communication skills. The role of the SE, like the role of the PM, requires strong leadership ability and emotional intelligence (Thomas 2011).

TABLE 1. FDA PROCESS RECORDS

FDA REQUIREMENT	PROCESS RECORD/ DELIVERABLES	RECORD OWNER
Design and Development Planning	Project Plan	Project Manager (PM)
Design Input	Voice of Customer (VOC) Risk Management (Hazard Analysis) Regulations Product Requirement Spec (PRS) System Design Document (SDD)	Systems Engineer (SE)
Design Output	PRS Verification and Validation Plan Project Plan Technical Outputs (e.g., drawings, schematics, etc.)	SE PM Engineer
Design Review	System Requirements Review (SRR) System Architecture Review (SAR)	PM Coordinates SE Reviews
Design Verification	PRS Verification and Validation Plan Detailed Verification Plan	SE Creates PM Oversees
Design Validation	Validation Plan	Typically Performed by Clients
Design Transfer	Project Plan	PM Plans and Coordinates
Design Changes	Engineering Change Order (ECO)	Engineering PM Approval
Design History File	Combination of the above items into cataloged directory	PM and SE Approvals

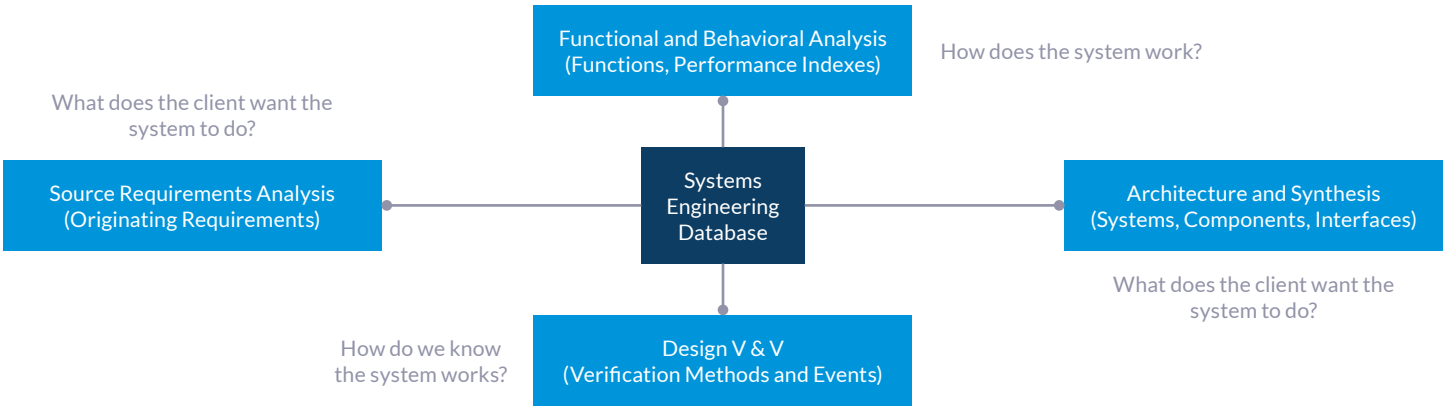
MBSE adds a reduced workload and full traceability to the regulatory compliance equation over nonmodel-based approaches. Two of the most complex documents listed in Table 1 (the PRS and SDD) are direct outputs of the MBSE database. Once the database has been established, updates can be quickly made and propagated throughout the design control documents without concern for conflicts. Moreover, the full traceability provided by MBSE tools (such as Cameo) between requirements, architecture, functions, and verification activities means that the design team can be confident in their compliance in the event of an audit. Figure 2 shows this traceability framework graphically.

While the focus of this paper, and specifically this case study, is on regulatory compliance associated with development within the United States, it should be noted that the process may be extended easily to development in other countries. Most Asian and Asia-Pacific medical regulations are based on FDA requirements and follow the model described in this paper. In Europe, because of efforts toward communization of regulations, there is an increasing correlation between FDA and ISO requirements. In some cases, we found that there is a need to align unique regulations (MDD/MDR, for example) with the FDA. One method to address this is to capture all requirements from this additional regulatory agency into an MBSE repository (such as Cameo) and then correlate the requirements one-for-one with the previously captured and mapped FDA requirements. MBSE significantly eases this correlation burden by tying the requirements directly to the verification activities planned for development.

Alternative, non-MBSE repository tools are also widely available and may be used on projects. It has been our experience that these tools do not fully envelop the definition of the product and thus require additional systems engineering tools (often paper-based) to complete system definition. The separation in tools thus results in a higher likelihood that changes occurring through the product development cycle will not be captured and propagated throughout all tools used on the project, resulting in potential discrepancies in SE documentation.

MBSE, as proposed in this paper, addresses the key FDA requirements for design controls during system development. Using the tools described above, Client A took a Class I medical device from concept through to full production in less than twelve calendar months. On this twelve-month project, only a fraction of the man-hours (less than 10 percent) was devoted to systems engineering. However, the design team was confident of FDA-compliant design controls because of the traceability provided by MBSE. The team was also confident that the market-appropriate product would be designed, developed, and produced at the desired cost, on time and within budget. It is our experience that a medical device development effort using the SE–MBSE process may take 12 to 20 months as compared to the same effort taking three or four years without the SE discipline. This same trend has been documented by Gardner (2001). A noted efficiency gained by implementing systems engineering, and especially MBSE, is the reduction in the need for retests because of late-entry requirements found during verification tests or field validation.

FIGURE 2. MBSE MODEL TRACEABILITY



THE CASE OF CLIENT "B"

Client B produces measurement devices for use in explosive, industrial environments. ALTEN Technology was engaged by the client to lead a multidisciplinary team through the definition of a common platform which could be leveraged across the design of multiple products. In addition to definition of the common platform, the client had not been introduced to systems engineering; part of the project was the introduction of best practices to the client team through leadership of the systems engineering process for one full development cycle.

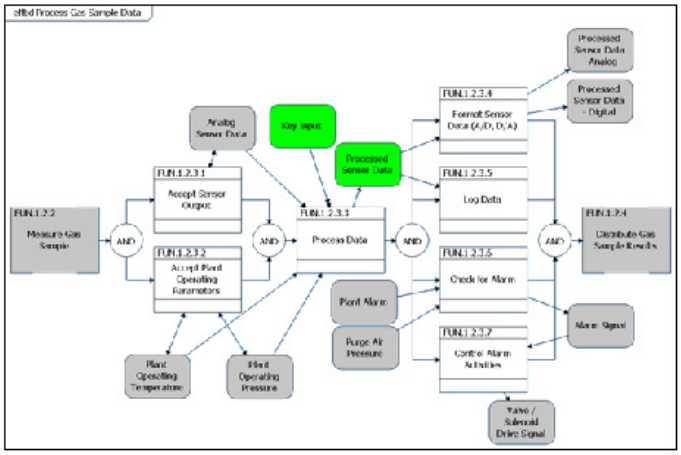
Initial discussion with the client uncovered that it had not significantly changed its product base for many years. While there were many reasons for its reluctance to make changes, two of the major drivers were (1) concern about regulatory compliance, and (2) concern with product field failures. Introduction and application of the systems engineering process focused the team's efforts on tasks required for definition of this common platform. MBSE provided the means to capture in one cohesive model the regulatory requirements, system use cases, functional requirements, and verification activities.

Client B was right to be concerned with regulatory compliance. Its products fall within the complex regulatory environment of explosive atmospheres (both gas and dust). These environments are regulated by multiple bodies dependent on the country, with the IEC 60079 series of standards representing the closest to a universal set of requirements available (IEC 2010). The common platform (and any design effort) needed to fully conform to eight complex IEC standards as well as multiple, parallel standards from other governing bodies such as the Canadian Standards Association (CSA) and the American National Standards Institute (ANSI).

Model-based systems engineering allowed for the creation of a master verification plan that could be applied to all future products. This was very appealing to the client which reported past experiences with significant predictability issues because of V&V failures or post-launch redesign efforts. Using our MBSE tool, we decomposed each of the key specifications section by section, requirement by requirement. This produced a fully traceable and searchable requirements tree. Using the MBSE database as a regulatory management tool, we could map parallel or repeated requirements to a common, single requirement and standards could be filtered from the specification on demand. Once we had decomposed the specifications, we created verification activities and mapped them to the requirements until all requirements were verified by some means. These verification activities ranged from keeping data sheets on file to design reviews to physical tests. In the end, MBSE allowed for the creation of a list of verification activities, tied to specific standards, which fully tested the product to the standards and can be leveraged on future projects. Moreover, the process gave the team confidence that new designs could meet the complex regulations. Another benefit realized by this system model approach is the output of the model as a superb input to third-party certification groups.

We alleviated concerns with product field failures during the project via similar means. Client B had an existing list of verification activities that had historically been done on new products, but which were not linked to functional requirements. As part of the project, enhanced functional flow block diagrams (eFFBD) were created to graphically document the intended functions of the product. These functions were then mapped to new, function-specific verification activities. Figure 3 shows an example of an eFFBD. This exercise highlighted many features and functions that had never been formally verified on the existing products; some of which had led to client product returns in the past. The emphasis on functional flow also served as a key tool in the development of the actual physical component common architecture. More information about using MBSE for common physical architecture development can be found in Gardner (2001).

FIGURE 3. ENHANCED FUNCTIONAL FLOW BLOCK DIAGRAM (EFFDB)



When the functional and regulatory verification activities were combined into a cohesive verification plan, the client had a clear picture of the steps required to confidently launch a new product. Because of the extensive regulations, over 300 individual requirements were identified for the common architecture. However, this list of requirements only led to approximately 60 verification events, encompassing everything from required design reviews and calculations to actual, physical testing. Even more importantly, thanks to the traceability provided by MBSE tools, when questions arose during certification, Client B could provide clear, logical explanations of the verification completed as well as the proven acceptability of the design. In addition, the client has seen great value in now being able to accurately predict the time and cost of accomplishing V&V.

Initial preparation of the common architecture required approximately five calendar months and twelve man-weeks to complete. The effort has led to a significant decrease in expected product development time with an estimated three-month reduction in development time per product. Additionally, the common system model requires very little reworking for each new project and can be updated in a matter of a few weeks for the development of a new product.

In comparison to alternative systems engineering tools such as nonmodel-based parametric databases and traditional paper-based tools, MBSE has allowed for a single database to completely define the system. This allows for the changes made in one area of the model to propagate through all deliverables associated with the systems engineering process. This is of particular importance and benefit in the development of products for highly regulated environments because regulations often change and lead to updates required in system definitions. Use of nonlinked and paper-based tools requires identified changes to be made uniquely and separately to the deliverables associated with system definition and does not give any feedback on whether the changes were implemented in a common manner or completed across all deliverables associated with the definition of the product.

Looking forward, Client B intends to sell into a new set of regulations that will make MBSE an even more vital part of their development efforts. To increase plant safety, IEC developed the 61508 family of standards which define the required design controls for functional safety of electrical, electronic, and programmable electronic safety-related systems (IEC 2010). This set of standards is like the FDA requirements of Title 21 in that the standards do not focus on mandating design constraints but instead define a set of design controls and process that should be followed. In another parallel to FDA discussions, adherence to the IEC 61508 standards is proven primarily through a quality audit of the design documentation as well as the enterprise quality system. Table 2 shows the high-level design control requirements of IEC 61508 and is based on IEC (2010) and Medoff et al. (2010).

As shown in Table 2, most of the required design controls are the responsibility of the SE. Similar to the discussion regarding Client A, MBSE tools allow for concrete proof of compliance with the standard and, in the event of an audit, full traceability between the separate process records.

TABLE 2. FUNCTIONAL SAFETY DESIGN RECORDS

IEC 61508 Requirement	DESCRIPTION	PROCESS RECORD / DELIVERABLES	RECORD OWNER
Functional Safety Management Plan	Develop a documented plan for project management as it relates to safety functions	Project Plan	PM
Product Safety Requirements	Capture the safety integrity level requirements and list the safety functions of the device	Originating Requirements Risk Management (Hazard Analysis) Regulations Product Requirement Specification (PRS)	SE
Safety Validation Test Plan	Create safety validation test plan mapped to safety requirements and functions	PRS Verification and Validation Plan Detailed V&V Plan	SE
System Architecture Design	Clearly define architecture and identify interfaces; analyze failure modes	System Design Document (SDD) Failure Modes and Effects Analysis (FMEA)	SE
Hardware Design and Implementation	Perform standard-specific tests such as component derating; ASIC requirements and fault injection are always required	Drawings, schematics, reports IEC-specific fault injection and FMEDA analysis	SE PM Oversees
Software Design and Implementation	Outline proper software engineering practice	Software Architecture Specification (SAS) Software Design Specification (SDS) Software Analysis	Software Engineer
Integration and Safety Validation Testing	Execute integration testing of hardware and software components	Detailed Verification Plan and Report (DVP&R)	SE
Process Validation	Final, internal audit of process records for completeness	Audit Report	PM

ABOUT ALTEN TECHNOLOGY

ALTEN Technology is an engineering services company that provides innovative solutions for engineering, IT, and product development projects across the product life cycle. For decades, ALTEN Technology has been helping clients develop products that are changing the world. We provide support across industries including aerospace, defense, automotive (including commercial vehicles), medtech, life science, rail, energy and environment, robotics, and unmanned systems.

CONCLUSION

Whether working in the FDA-regulated medical field or explosive industrial environments, using MBSE provides the confidence, traceability, and structure to meet regulatory requirements, optimally develop the right product, and cost-effectively prove compliance. In addition to the MBSE advantage, we propose that combining the roles of the PM and the SE cost-effectively aids regulatory compliance. Client A found that use of MBSE as proposed in this paper efficiently produced the required design controls for FDA regulatory compliance, resulting in very low systems engineering costs (fewer than 10 percent of the project hours) without sacrificing confidence in the quality of its DHF. For Client B, MBSE has provided a reusable roadmap for compliance with complex, parallel standards in the explosive atmospheres environment. Both clients gained a real, quantifiable advantage by using the proposed systems engineering approach to tackle design in regulated environments.

REFERENCES

"Explosive atmospheres — Part 0: Equipment — General requirements," International Electrotechnical Commission (IEC), IEC 60079-0 ed6.0.

"Functional safety of electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission (IEC), IEC 61508 ed2.0.

Gardner, J.R., 2001. "Design of a Common System Architecture for a Medical Device Application," Paper presented at the 11th Annual International Symposium of the International Council On Systems Engineering — INCOSE, Melbourne, Australia, Paper P104.

FDA, 2010. "Good Manufacturing Practice for the Medical Devices," Code of Federal Regulations 21, Part 820. Food and Drug Administration. Revised April 1, 2010.

Haskins, C., ed. 2010. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. Version 3.2. Revised by M.

Krueger, D. Walden, and R. D. Hamelin. San Diego, CA (US): INCOSE.

Kasse, T. 2003. "The Differences Between the Project Manger and the System Engineer." Paper presented at the 6th Annual System Engineering Conference - NDIA, San Diego, CA (US), 10-23 October.

Kolozs, J., Henderson, C., Gardner, J., 2012. "Systems Engineering Lite." Paper presented at the 22nd Annual International Symposium of the International Council On Systems Engineering — INCOSE, Rome, Italy.

Medoff, M.D., Faller, R.I., 2010. Functional Safety – An IEC 61508 SIL 3 Compliant Development Process, Exida, Sellersville, PA.

NASA, 2011. NASA Project Management and Systems Engineering Competency Framework, www.nasa.gov/offices/oce appel/ pm-development/pm_se_competency_framework.html, Accessed on Nov. 4th 2011.

Thomas, J.A., 2011. "Wanted, System Engineers with Moxie," Presentation, http://community.vitechcorp.com/forum/default.aspx?g=posts&t=67, Accessed Nov. 4th, 2011.