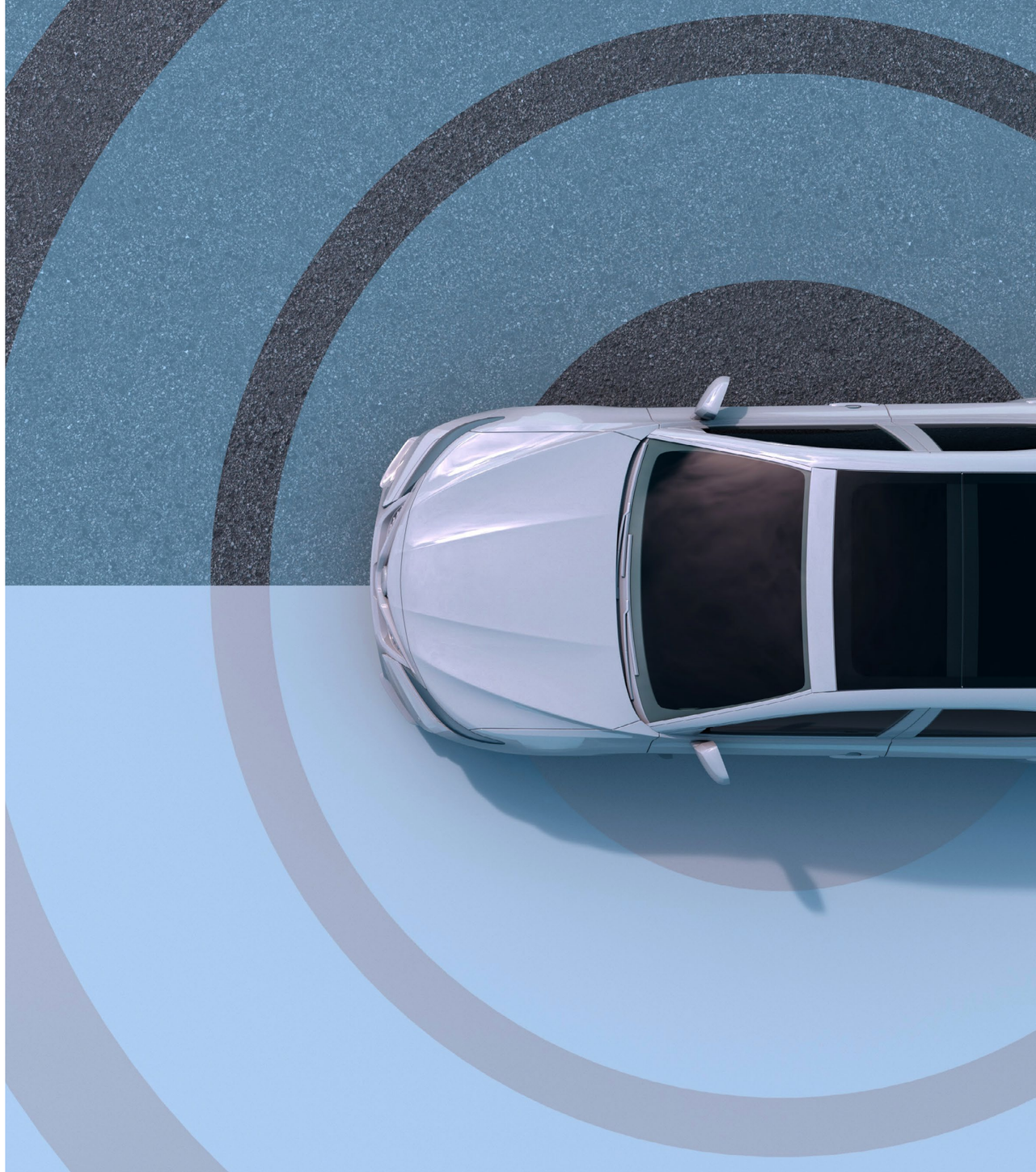
SOFTWARE INTENSIVE SYSTEMS | WHITE PAPER

Safer deployment of automotive innovations

The future of the automotive process

LET'S GO



Safer deployment of automotive innovations requires trusted, agile processes

Embedded and systems software is driving a great deal of automotive technological innovation. Electronics for control and sensing use machine learning to accelerate insights into usage patterns. Product upgrades now occur over the air in the consumer's driveway instead of at the dealership, providing a constantly optimizing product. Consumer interest in electric vehicles is expanding beyond the early adopters. Vehicle electrification requires replacing conventional powertrains with electric drive units, batteries and harnesses.

In addition, automotive business models are changing. New players have entered the marketplace, promising attractive products. Developing advanced driver-assistance systems (ADAS) and autonomous technologies requires close and continuous collaboration among product management, engineering, supplier management, IT operations and many other historically siloed corporate groups. Processes are refining to encourage collaboration among historically separate automotive disciplines.

How does a company keep pace while demonstrating the safety and security of its products? Existing and emerging industry standards help all disciplines address risks at the relevant speed of innovation. They include ISO 26262 for functional safety, ISO 21448:2022 for Safety of the Intended Function (SOTIF), and ISO/SAE 21434 for vehicle cybersecurity. Moreover, new players need to understand how to get the most out of established standards, such as IATF 16949 (based on APQP), and how Automotive SPICE® can help improve the quality of complex software and systems.

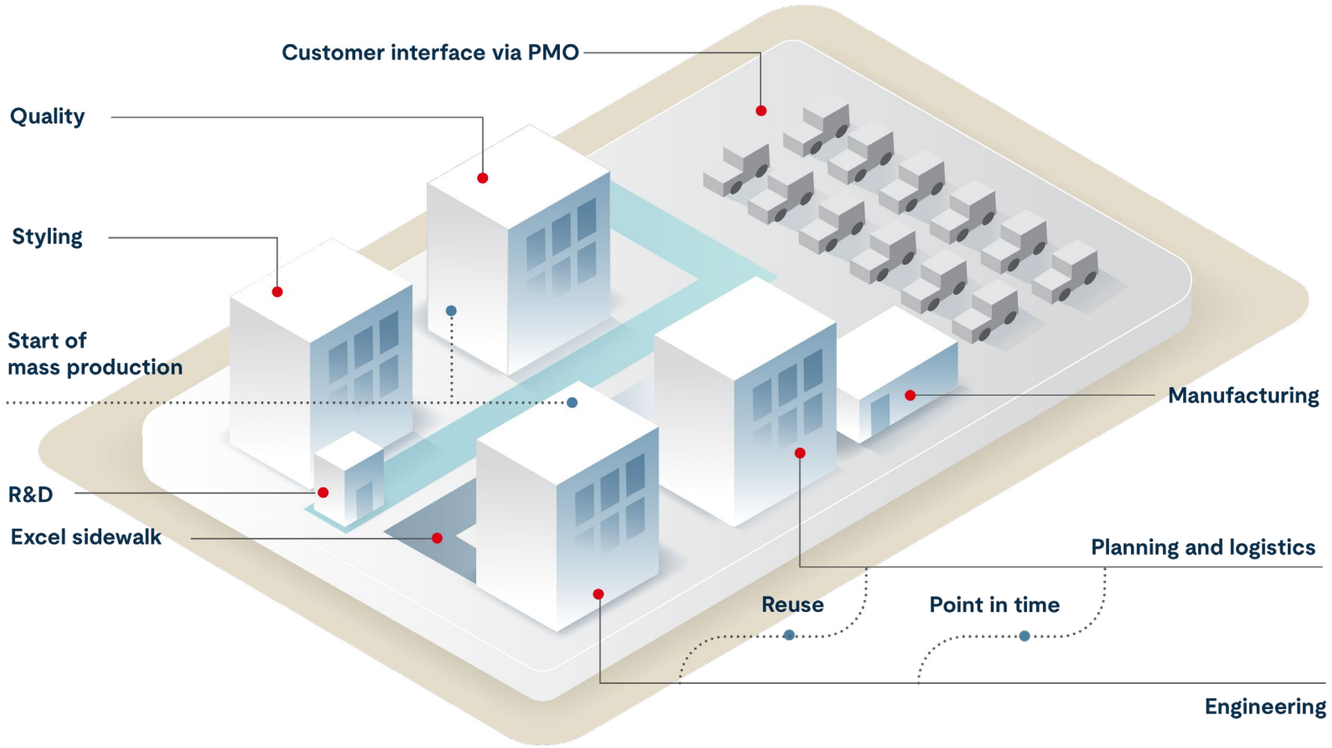
In this white paper, we will discuss how all of these challenges interconnect and have a common denominator: the processes used to manage the products across their life cycles. Consumers need to be able to trust those processes for safety and security, and the processes need to be agile to cope with the pace of innovation and shifting consumer demands. Process management software Stages provides a process framework to model a corporation's decision progress and compliance so the user can see to see how the company's process complies with multiple standards.

Product development process baseline

Stages offers a sample framework of a product development process (PDP) to demonstrate the software's ability to capture and manage the decision's progress in a large manufacturing company with many different actors. This PDP continuously undergoes enhancement — just like what might happen in a real learning organization — with the goal of using the process model as a basis to establish standards compliance. Stages associates standards elements with process elements, thereby creating a link showing how and when an organization addresses standards. As processes are used on new products, instantiation or tailoring often occurs based on the organization or market demands.

Figure 1

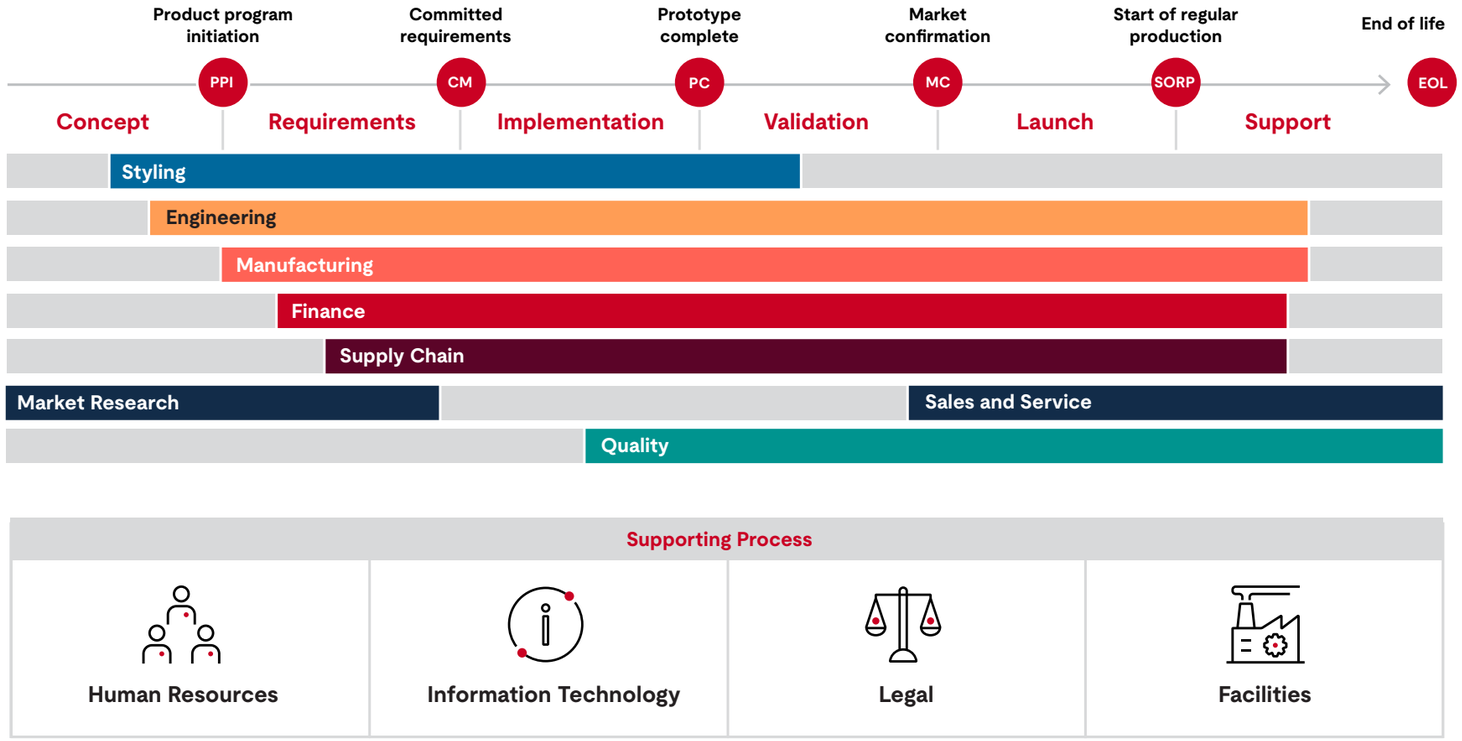
Visualization of decision processes within an organization



Figure

2

Visualization of decision processes within Stages



Automakers are delivering faster innovation

Innovation speed often drives competition. Agile methods that keep the customer's interests and desires at the forefront yield faster development. Manufacturing maturity is often captured in a bill of process (BOP) that helps establish predictable quality. The same mindset applies to decision-making and managing risk when developing and introducing new technology into the marketplace. Stages helps a product execution proceed based on a proven process that has evolved over time. The evolution may be driven by lean principles and quality insights. It can also be driven by a disciplined scientific discovery process when advancing new technologies, e.g., batteries and power electronics in automobile applications.

Consumers and governments want innovations and to keep products safe. How can these potentially conflicting challenges be addressed? The key lies in the fact that they are interconnected and have a common denominator: PDP. The processes used to manage development progression need to consider regulatory elements in the context of the base product development rather than an end-of-line quality check. Certification often requires evidence that a measurement standard has been achieved and that product safety due diligence was performed. This should be accomplished as the development plan is executed. Specific plan deliverables are directly associated with standards and regulations, helping engineers make the best timely decisions.

The product plan comes from the corporate experience, which is the PDP. Stages can associate standard elements with process model elements, making the specific parts of a standard visible in the context of who, when and what, and providing the why. The process owners and regulatory experts work together to confirm that product engineering and manufacturing address all required standards. Even seeing this in R&D scientific method practices would boost the discovery pace of innovations with safety in mind from the start, which can help organizations focus on safer innovations.

Navigating compliance while innovating

Standards are not regulations

Engineering experts often develop standards in areas where systemic failures occur. A good standard provides a measurement technique to help decide what conforms and what doesn't. Such measures improve quality by narrowing variation. With variation in mind, many manufacturers start thinking of statistical process control (SPC), which is required in standards such as IATF-16949 for automotive quality management systems. Some regulations refer to industry standards that must be used to establish that the product was engineered and produced with safety in mind.

However, SPC applied to a unique part or product during engineering does not apply in small sample populations. A sequence of decisions with timely risk management assessments can help in the development of new products. Techniques such as Failure Mode and Effects Analysis (FMEA) augment SPC (rate and frequency of nonconformance) with a failure probability, which leads to a risk score. The engineering process measures the product risk, typically in a peer review, and decides what to do based on historical experience. In Stages, the PDP model has techniques such

as FMEA as a simple workflow used once a design has been chosen. It is a reactive risk management practice. SPC can be applied by looking at the results of all FMEA workflows across different products and examining the correlation with improved product durability and safety. Insights from this kind of process comparison lead to effective process improvements. These improvements can drive efficiency and safety together, rather than as independent initiatives.

Stages enables the visualization of development decisions in the context of standards and regulations, thereby helping to mitigate risk. This can be done by searching for key phrases used across the PDP or associated with work products and guidance within Stages.

Safety standards need visible compliance

Safety standards, e.g., ISO 26262, and supply chain standards, e.g., IATF 16949, drive a company's processes. One focuses on the discipline of managing and improving mass production with supply chains, while the other focuses on functional safety. Companies need both standards represented in the processes and, when required by a certification agency, they need to provide evidence of compliance. Figure 2 shows how ISO 26262 standard elements are visible in the context of the work product "Corporate Regulatory Guidance," modeled in Stages. Note the context of activities producing and consuming the work product.

Modeled practices from IATF 16949 can be found directly in the PDP, as well as in the FMEA and the Design Verification Plan and Report (DVP&R). In these two cases, the guidance captured for the method simply refers to the Advanced Product Quality Planning (APQP) standard for a definition and explanation of these elements. Establishing the link to formal definitions and practices, especially when they come from industry standards bodies, helps contextualize what is important in the product development process: the next decision, keeping manufacturing in mind. Using Stages' search capability, one can quickly find references to common terms like APQP, FMEA and DVP&R. Some are just terminology, while others are methods for assessing risk. In many cases, regulatory bodies require evidence — a work product that is under version control and available to authorities upon request.

In mature companies, a role like regulatory engineer is responsible for monitoring all of these regulations and standards and preparing policy updates to outline the best way to satisfy the regulations. This role works with the sales manager to understand certification requirements at the point of product sale/delivery.

The PDP model defines "regulatory engineer." This individual's job is to stay aware of and summarize corporate policies to satisfy point-of-sale regulations. The deliverable is then provided to the rest of the engineering team. The Corporate Regulatory Guidance work product in this view is the same work product as in the previous view. These are different contexts, also known as different views of the work product. These multi-view contexts, shown on demand, are one of the benefits when expanding model-based processes from one discipline across the broader enterprise.

Figure

3

ISO 26262 standard within the work product “Corporate Regulatory Guidance”

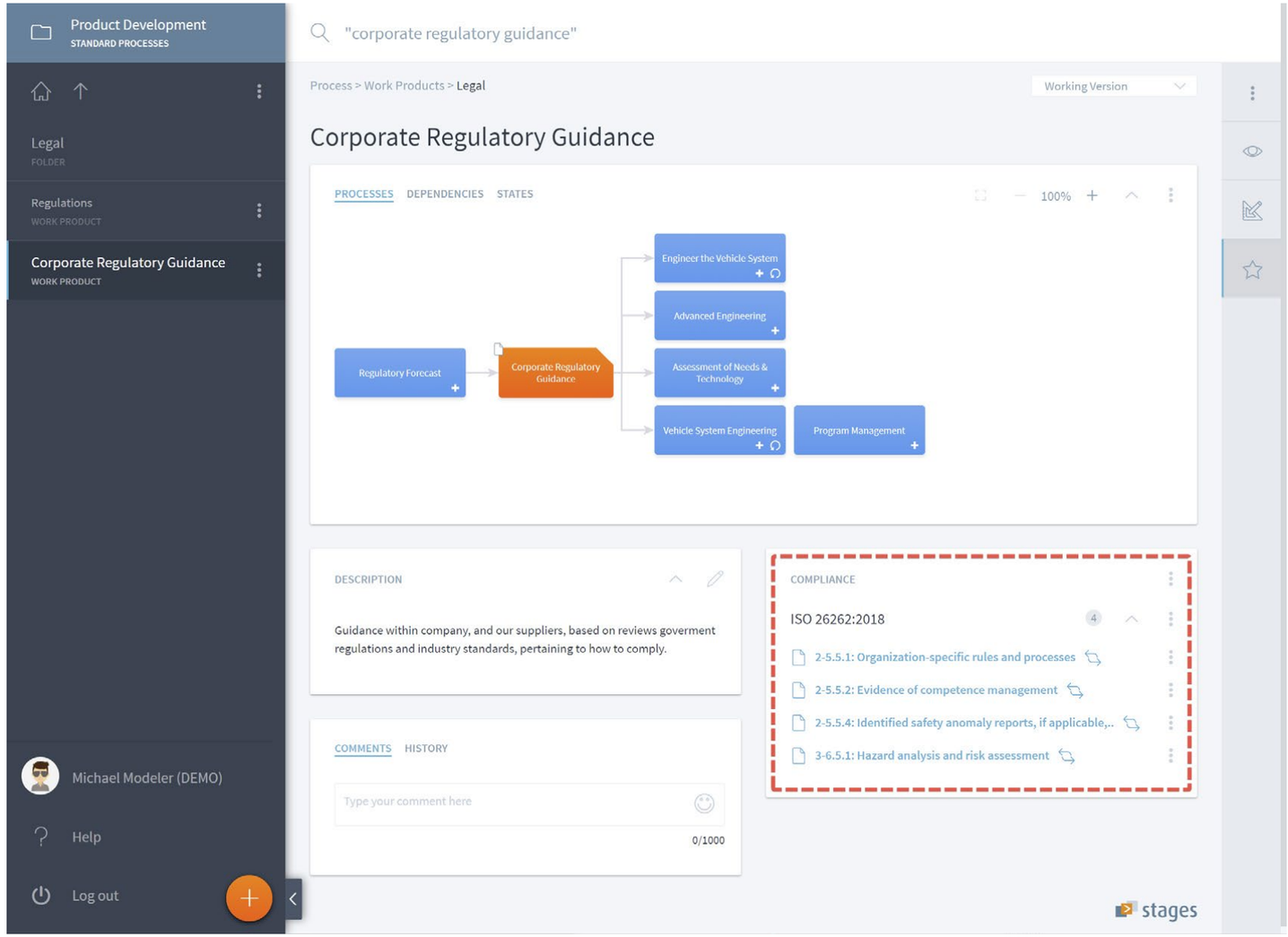
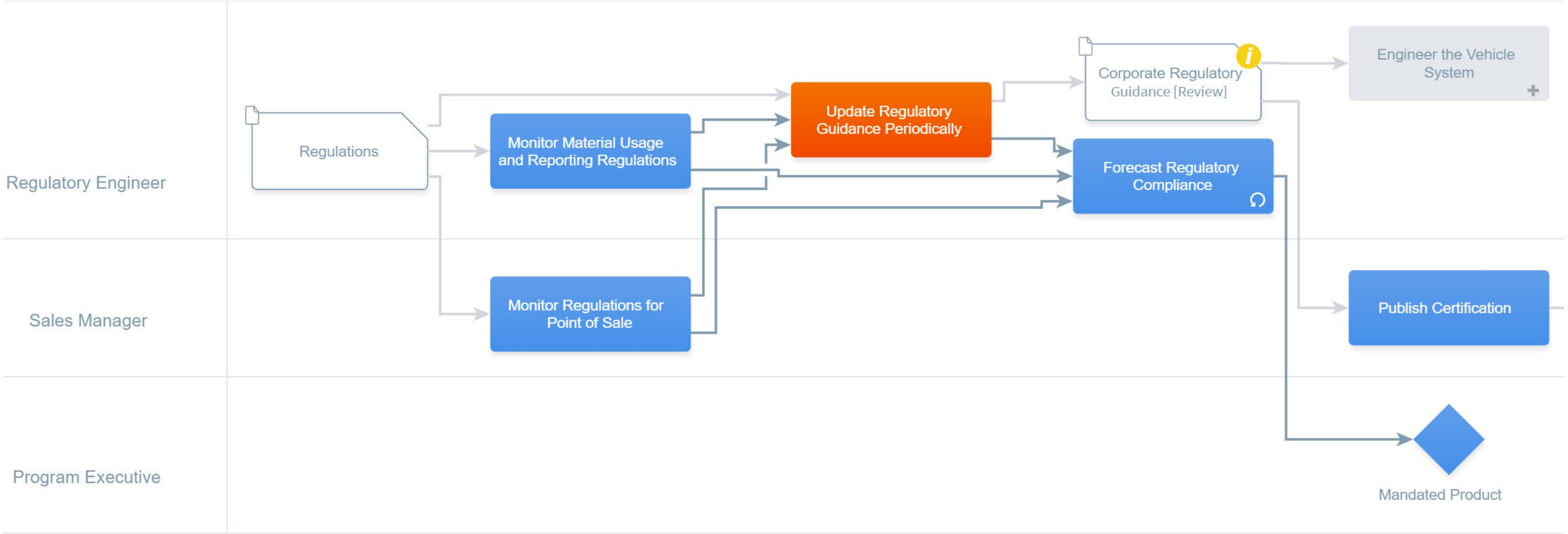


Figure 4: Interaction of a regulatory engineer, sales manager and program executive



Managing overlapping, conflicting standards

Some standards clarify terminology, which improves understanding, sometimes leading to regulations. Defining criteria for regulation-mandated certification requires the measures and techniques to agree in order to achieve compliance and confidence. As the world becomes more complex, safety experts use process assessments to evaluate the safety of product operation. This is often driven by consumers and their advocates such as insurance companies and governments wanting to improve public safety.

Standards and the related regulations can overlap and even conflict as you consider a global product sold in different regions, each with its own regulations. Seeing development decisions in the context of standard and regulation elements helps lower risks. Consistently performing the same sequence of steps leads to standards of work. A work product, such as a safety analysis report (Figure 4), shown in the context of the decision progression, can help people understand the conditions of successes and failures.

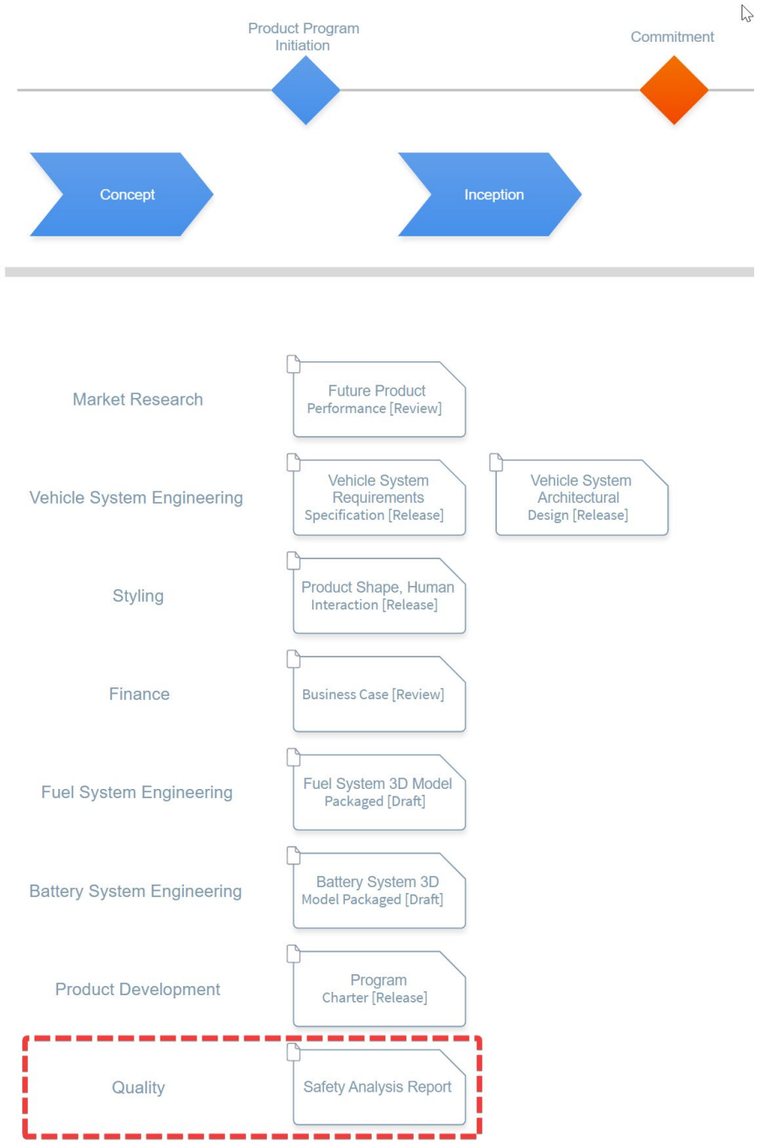
People want control of their work so they can develop improvements. It is human nature to improve through learning, but it becomes overwhelming when there are more and more standards and regulations to consider.

Stages has a compliance feature that manages the complexity of satisfying many standards and regulations simultaneously. The focus is on the proven processes, with managing standards frameworks in the background. Figures 5-8 show views of what this looks like using the tool. Figure 6 shows a view from a different reference model created to support ISO 26262. The evolution of the PDP model could copy roles from a reference model or, more likely, enhance existing roles to include the standards-driven responsibilities. Displaying the link to specific standards requirements is the key to making sure the PDP evolution remains compliant with standards. Figure 7 is an example of different standards requirements supported by a single element in the process model. Figure 8 shows an example compliance report, which helps the process modeler to assess the completeness of the process's coverage to specific standards.

Figure

4

Relevant standards for an automotive safety analysis report



Figure

5

Activity with functional safety standards compliance added to quality discipline; note compliance association to ISO 26262

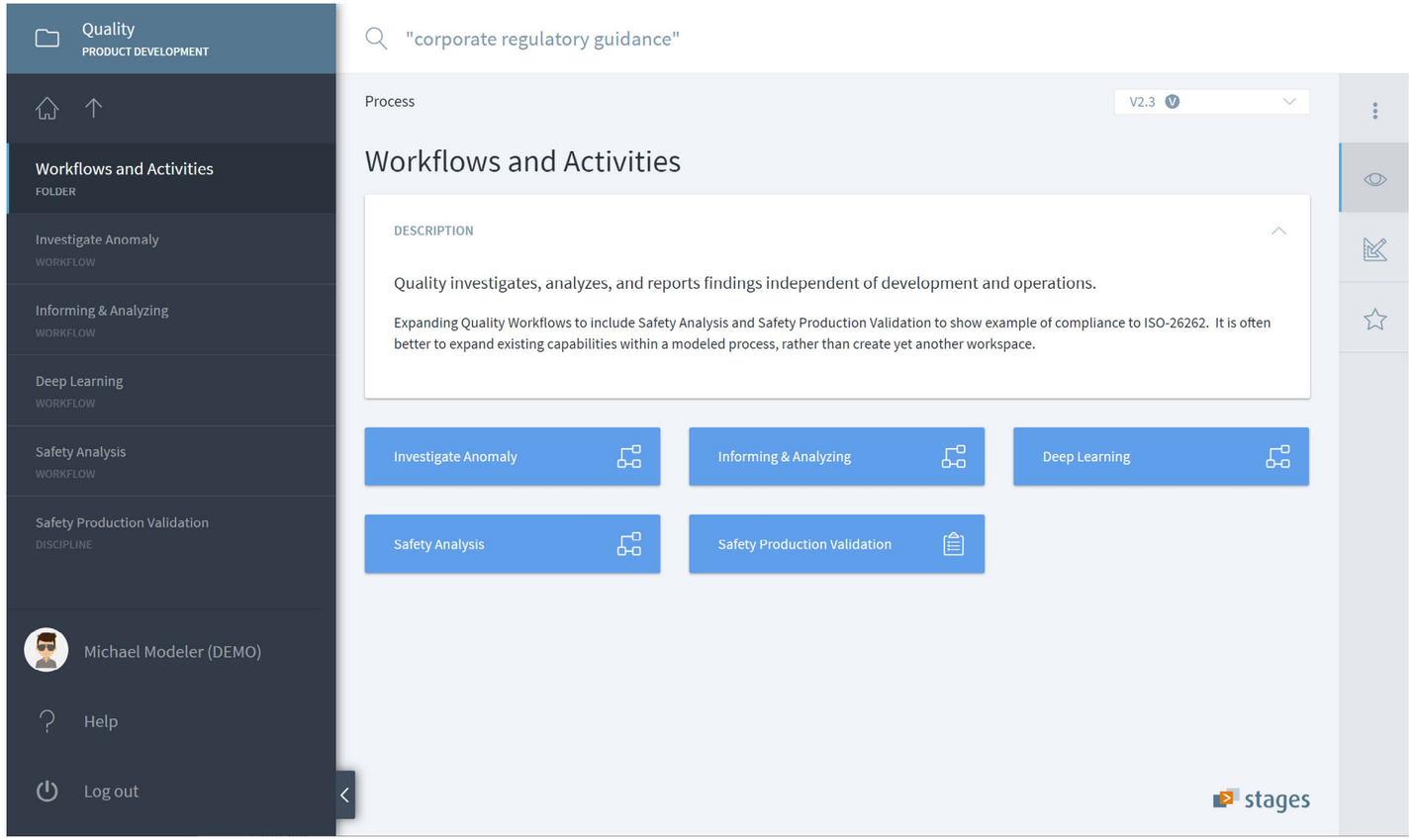
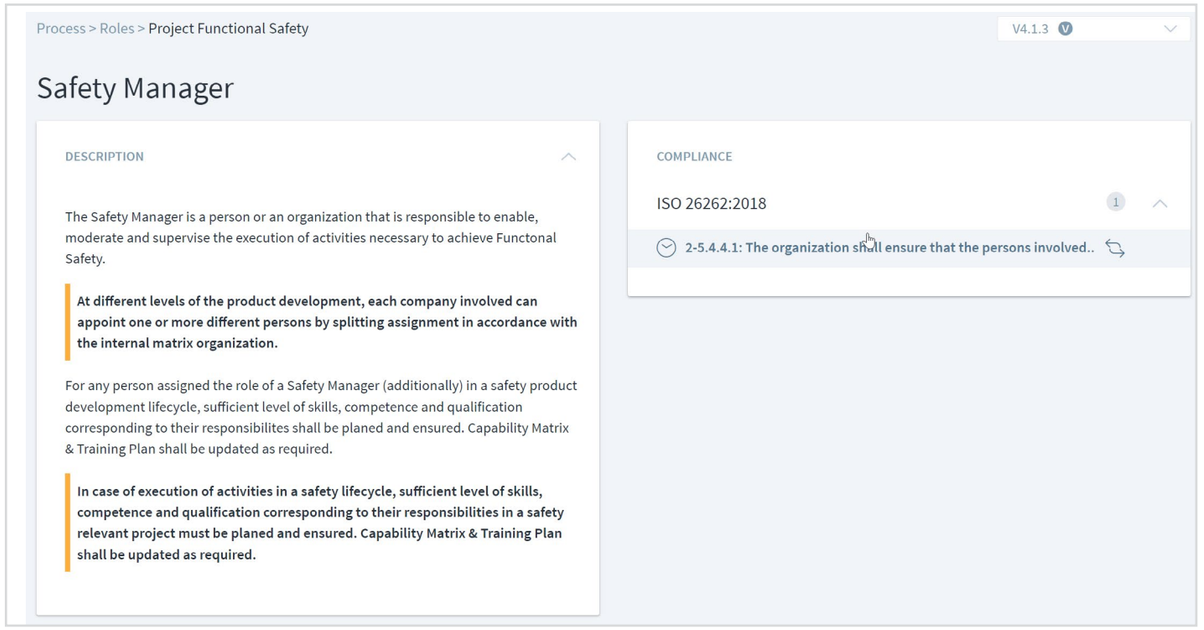


Figure 6: Roles identified in ISO 26262 shown in Stages Functional Safety Reference Model; note compliance link



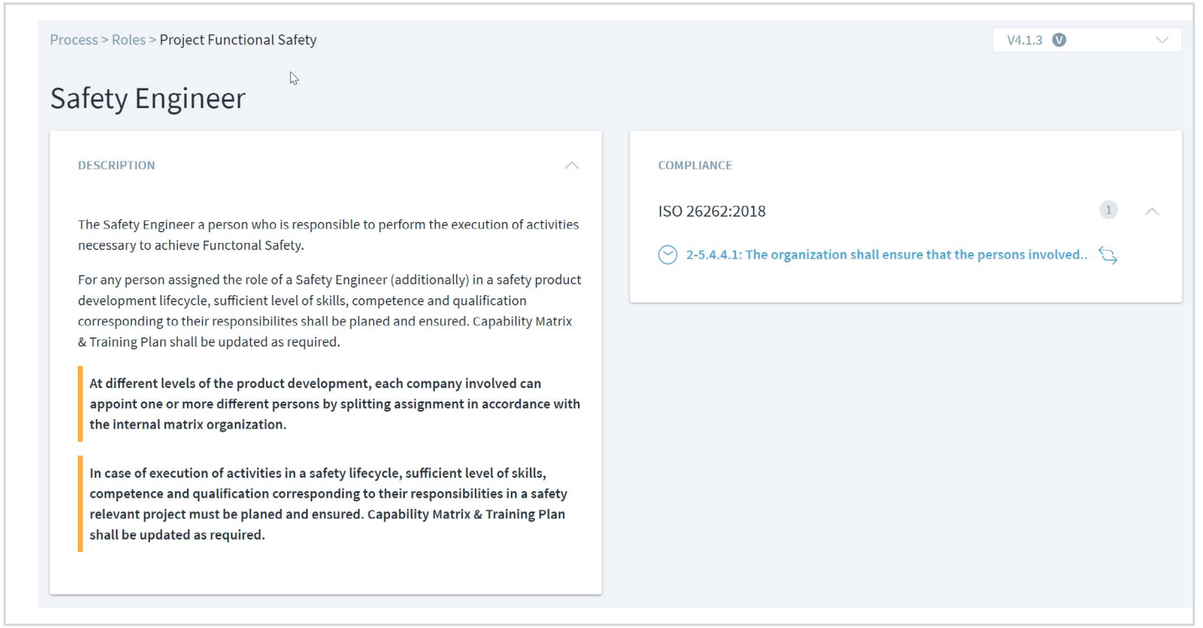


Figure 7: Multiple standards shown in context of existing process

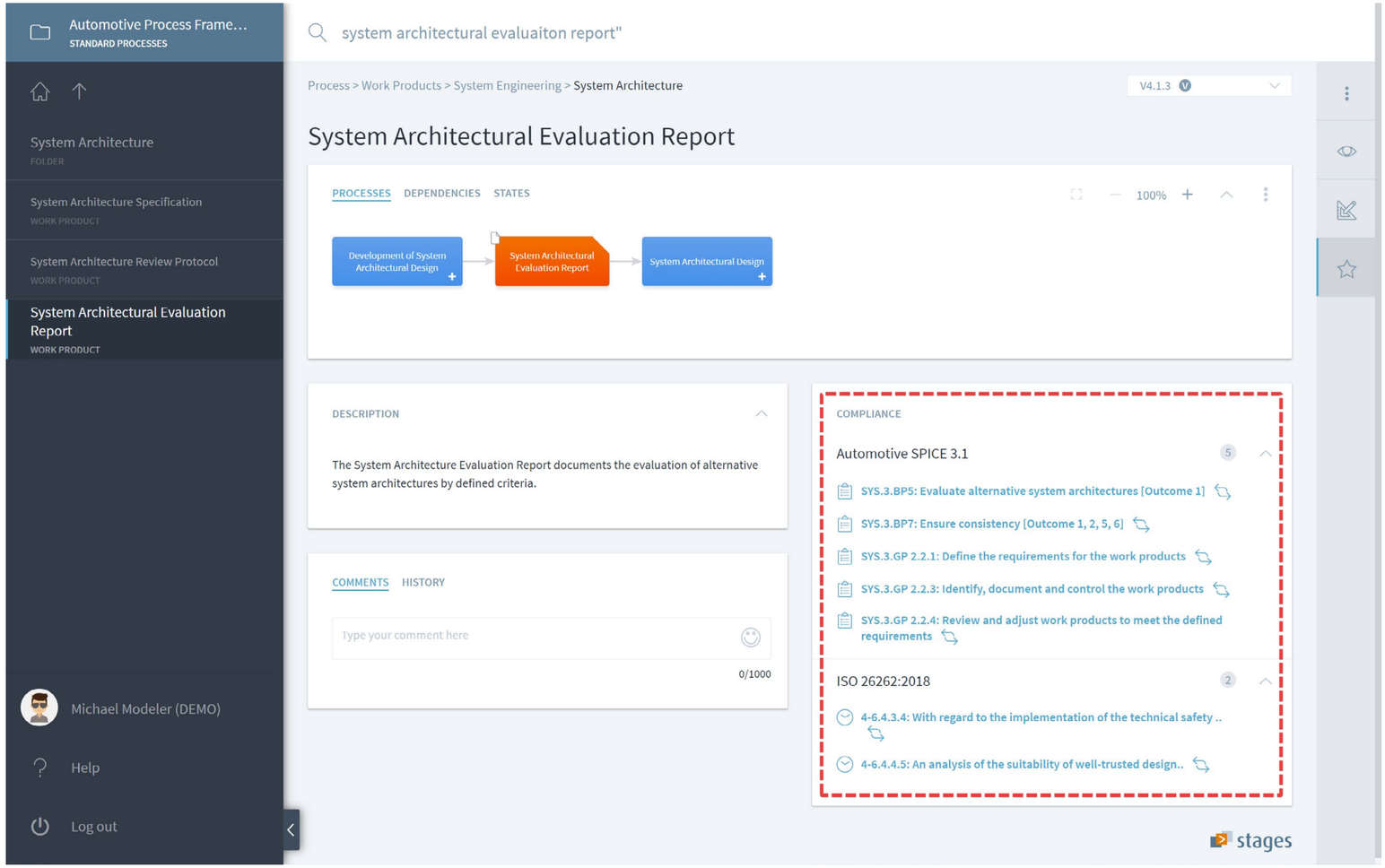
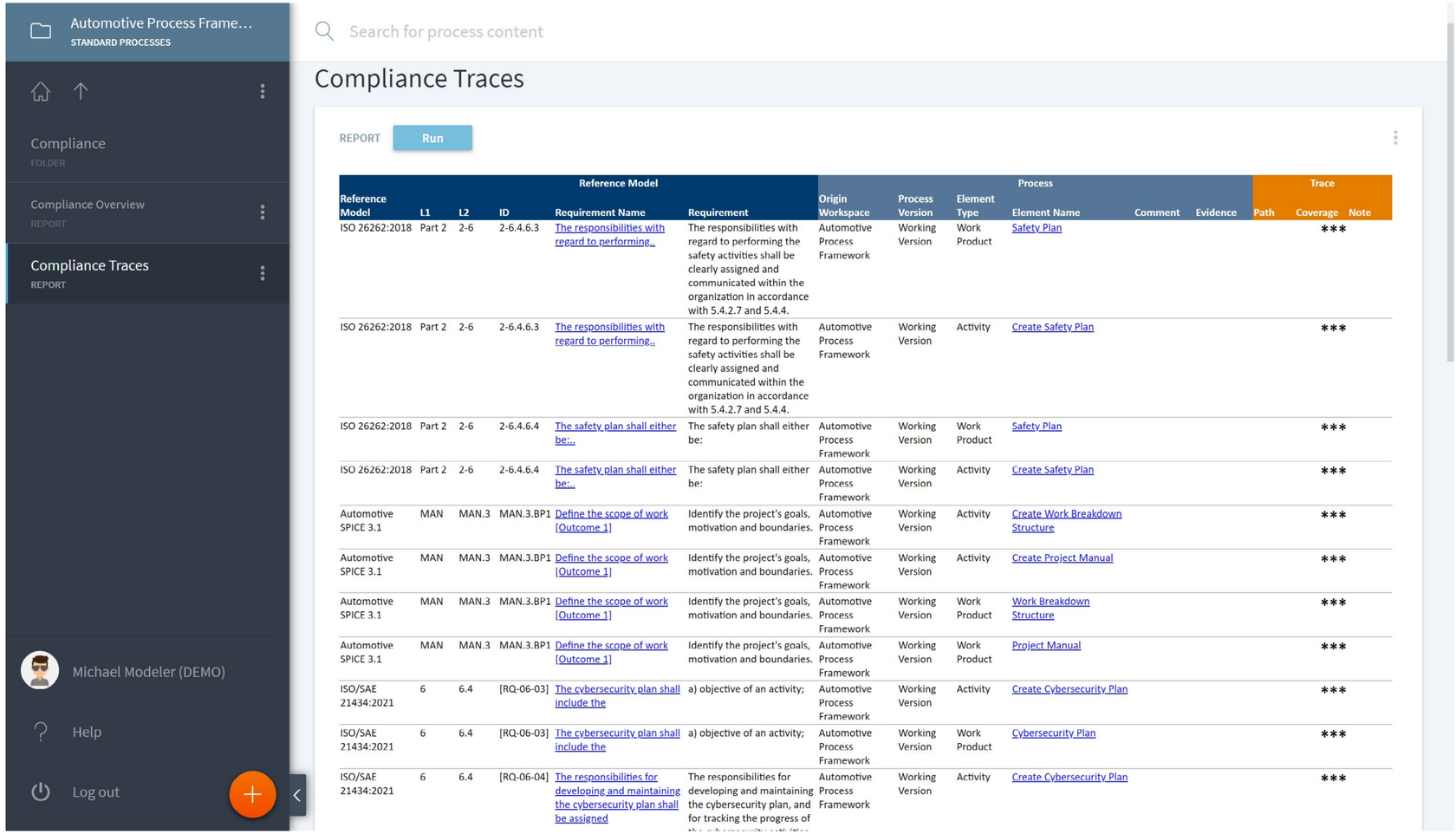
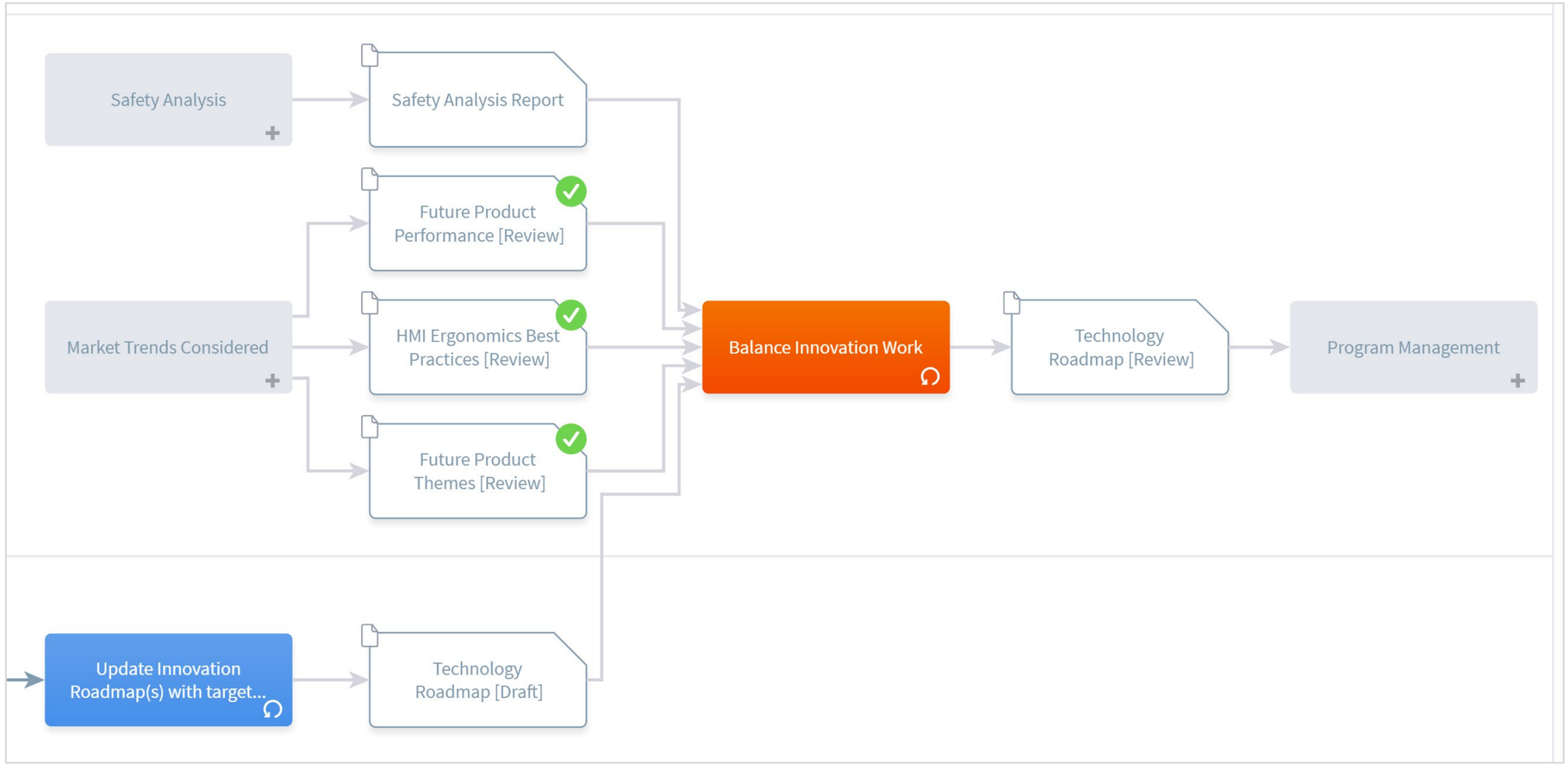


Figure 8: Reports of standards coverage and confidence



Reference Model						Process						Trace		
Reference Model	L1	L2	ID	Requirement Name	Requirement	Origin Workspace	Process Version	Element Type	Element Name	Comment	Evidence	Path	Coverage	Note
ISO 26262:2018	Part 2	2-6	2-6.4.6.3	The responsibilities with regard to performing..	The responsibilities with regard to performing the safety activities shall be clearly assigned and communicated within the organization in accordance with 5.4.2.7 and 5.4.4.	Automotive Process Framework	Working Version	Work Product	Safety Plan				***	
ISO 26262:2018	Part 2	2-6	2-6.4.6.3	The responsibilities with regard to performing..	The responsibilities with regard to performing the safety activities shall be clearly assigned and communicated within the organization in accordance with 5.4.2.7 and 5.4.4.	Automotive Process Framework	Working Version	Activity	Create Safety Plan				***	
ISO 26262:2018	Part 2	2-6	2-6.4.6.4	The safety plan shall either be:..	The safety plan shall either be:	Automotive Process Framework	Working Version	Work Product	Safety Plan				***	
ISO 26262:2018	Part 2	2-6	2-6.4.6.4	The safety plan shall either be:..	The safety plan shall either be:	Automotive Process Framework	Working Version	Activity	Create Safety Plan				***	
Automotive SPICE 3.1	MAN	MAN.3	MAN.3.BP1	Define the scope of work [Outcome 1]	Identify the project's goals, motivation and boundaries.	Automotive Process Framework	Working Version	Activity	Create Work Breakdown Structure				***	
Automotive SPICE 3.1	MAN	MAN.3	MAN.3.BP1	Define the scope of work [Outcome 1]	Identify the project's goals, motivation and boundaries.	Automotive Process Framework	Working Version	Activity	Create Project Manual				***	
Automotive SPICE 3.1	MAN	MAN.3	MAN.3.BP1	Define the scope of work [Outcome 1]	Identify the project's goals, motivation and boundaries.	Automotive Process Framework	Working Version	Work Product	Work Breakdown Structure				***	
Automotive SPICE 3.1	MAN	MAN.3	MAN.3.BP1	Define the scope of work [Outcome 1]	Identify the project's goals, motivation and boundaries.	Automotive Process Framework	Working Version	Work Product	Project Manual				***	
ISO/SAE 21434:2021	6	6.4	[RQ-06-03]	The cybersecurity plan shall include the	a) objective of an activity;	Automotive Process Framework	Working Version	Activity	Create Cybersecurity Plan				***	
ISO/SAE 21434:2021	6	6.4	[RQ-06-03]	The cybersecurity plan shall include the	a) objective of an activity;	Automotive Process Framework	Working Version	Work Product	Cybersecurity Plan				***	
ISO/SAE 21434:2021	6	6.4	[RQ-06-04]	The responsibilities for developing and maintaining the cybersecurity plan shall be assigned	The responsibilities for developing and maintaining the cybersecurity plan, and for tracking the progress of	Automotive Process Framework	Working Version	Activity	Create Cybersecurity Plan				***	

Figure 9: Safety analysis report added to advanced engineering activity: Balance innovation work, keeping safety in mind from the start



Summary

Future automotive challenges are interconnected and have a common denominator: the processes used to manage the products across their life cycles. Consumers need to be able to trust existing processes for safety and security, even as those processes need to become more agile to cope with the pace of innovation. A few samples from important standards are linked into the Stages PDP, which will continuously expand to cover operations and reporting.

Related content

For further content, including white papers and webinars describing the basic elements of PDP that have evolved from decades of experience and standards, like APQP and IATF 16949, and for more insights into Stages and product development processes (PDP), please visit www.ul.com/sis/stages/engineering-process-management.

Author

Craig Brown
Principal consultant
at UL Solutions

UL Solutions

UL.com/SIS

SOFTWARE INTENSIVE SYSTEMS

MCS24CS19809518