ptc

DIGITAL TRANSFORMS PHYSICAL

LÖSCH UND PARTNER GMBH

ISO 26262

Top 8 Blunders

Complying with ISO 26262 ‘Road vehicles - Functional safety’

ISO 26262 is an internationally recognized risk-based safety standard that regulates the functional safety of automotive electrical and electronic systems.

It ensures that a high level of safety is maintained, and is built into the components of a car from the very beginning. The purpose of ISO 26262 is to **address and mitigate possible hazards caused by malfunctioning systems in vehicles**. Complying with this standard helps automakers detect, manage, and/or mitigate the effects of system and hardware failures.

In the context of automotive development, compliance with this standard is probably one of the most important ones, as it **affects the whole engineering life cycle**. Therefore it is even more important to understand which blunders to avoid.

ISO 26262 in a nutshell

This eBook shares our experience of a successful implementation of ISO 26262.

As automotive companies usually do not struggle in the safety-specific domain, this eBook is about not safety domain-specific content (Dependability).

The addresses of this eBook are managers in the automotive company dealing with ISO26262. Hosted by Lösch & Partner's expert, this eBook provides our experiences and best practices in 8 Blunders and possible solution approaches.

Setting the context of ISO 26262

The complexity in the development of cars has massively increased and will continue to increase.

This is illustrated by the rise of the software code lines in the car. Today there are about 100 Million lines of code, while this was about 10 Million ten years ago. **But not only the complexity has increased but also the demands regarding safety issues.** Today cars need to have strong assistant systems to gain high NCAP ratings.

Let's have a more detailed look at the complexity. Complexity is measured as the sum of the requirements times the difficulty of the requirements times the product of the interdependencies.

- **The amount of code** has increased from 10 Million to 100 Million Requirements in the last 10 years. Regarding software guidelines on average 1 Requirement should be used for 25 lines of code. This means that the number of Requirements increased by a factor of 10 in the last 10 years and will keep increasing (See source: VW)

- Also, the **difficulty of the requirements** has on average increased. As new assistant driving systems and digital features have more complex requirements (Alejandro Saldo) and thereby slightly increase the average

- Due to the "digitalization" of the car, **the amount of interdependencies** has also increased as there are "connected components" and software instead of "isolated hardware components"

Sources: Euro NCAP 2020: Was ist neu beim Crashtest? | ADAC / So vernetzt sind unsere Autos | VW / The concept of problem complexity, Alejandro Salado / Value creation in innovation ecosystems

To sum up there is a massive increase in complexity.

To deal with it, car companies are in a transformation and introducing more sophisticated methods of working like System Engineering, SysML, and MBSE, new ways of working together like agile frameworks and agile methods, and new tools ...

ISO 26262 is the standard in the automotive industry trying to ensure quality, safety, and risks by giving ways to deal with the complexity and the increased demands in the safety area.

#1 Blunder: Have a good “foundation”

Do you have trouble managing the complexity? Is there a lack of traceability and are there a lot of silos? Do you not have common tools and common state-of-the-art processes?

If you can answer yes to these questions, achieving ISO 26262 will not be easy and will take a lot of effort. Additionally, gaining full benefits will probably not be possible. This could be for example several requirement management processes, separate processes for laws, or other top-level requirements. Also, this could be not using a holistic approach for requirements, software, testing, and architecture.

Solution: Use state-of-the-art processes & methods

Manage your complexity by having traceability from top to bottom, eliminating silos, and using company-wide, standardized & integrated processes and methods. The goal is to implement a set of mandatory workflows and artifacts within a tool, which represent company-specific processes that are currently used within the engineering-domain. This is not just useful to fulfill the ISO 26262, but also to gain efficiencies and reduce risks as well as time-to-market.

#2 Blunder: It's not just about safety

ISO 26262 is not just impacting safety expert domains but is closely linked to the entire product development process, such as requirements management, test management, and configurations management.

The safety experts are usually working full-time creating dependabilities and work artifacts and complying with ISO 26262. Nonetheless, this may not always be the case for other areas ("Forgottenland").

Solution: Create awareness and skills

Management attention and training on ISO 26262 compliance are essential to give managers, process and tool owners as well as developers the required skills to also align the "Forgottenland" processes accordingly.

A good way to start the deep dive is to organize workshops with cross-functional teams including safety experts, process owners, tool owners, and developers to get a holistic shared understanding, identify gaps and create a common roadmap. Afterward, start to integrate ISO 26262 and release relevant output into the processes and tooling.

#3 Blunder: Understanding ISO 26262

Understanding ISO 26262 is not trivial.
While experts can do this, understanding ISO 26262 is often not so easy for regular managers and developers.

Facts & figures on ISO 26262:

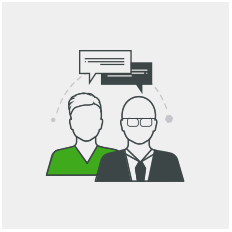
- **12 parts (1 adaptation of ISO 26262 for motorcycles)**
- **107 chapters**
- **690 pages**
- **>100 work products**

Thus, the solution of Blunder 2 recommended cross-functional workshops could lead to overburdening and therefore demotivation of individual participants. Therefore, engineers would need role-specific information & guidance on their relevant ISO 26262 parts.

Solution: Translate ISO 26262

Have an expert team translate the ISO 26262 into understandable segments & requirements for managers and developers - reduce information to key essentials and “snackable” content. At the same time, it is recommended to create transparency by providing an overview of all ISO 26262 impacted stakeholders.

Documentation and sharing of the reduced content is a second step to ensure the durability of the success. This is often achieved by the implementation of a shared knowledge management system (e.g. wikis, or communities of practice).



#4 Blunder: Do it right from the beginning

This seems to be obvious but however regarding our experience often ISO 26262 is not integrated in the core processes of the development from the start due to the initial workload.

Implementing the ISO 26262 activities as a separate process or even reengineering this after concluding the development, causes a lot of extra manual work, risk of changement costs and adds no to few benefits to the product.

Solution: Delegate implementation

In our experience, this works particularly well in agile environments where the team takes responsibility and one or two teams are assigned the task of implementing a pilot. “Communities of practice” can then help transfer knowledge.

Afterward, have the teams, experts and process owners implement the ISO 26262 activities into their processes and create the required work artifacts and reviews.

#5 Blunder: Use common processes

Using different processes and degrees of maturity reduces compatibility and fosters silos while reducing traceability. Especially departments handling several completely different processes (e.g. an ISO26262-compliant process and a non-compliant process) have difficulties in fulfilling the requirements.

Therefore, it might be a good idea to reduce the number of processes through standardization. Heterogeneity seems to be one of the biggest blunders.

Solution: Optimizing processes

To reduce the number of silos, it is necessary to jointly analyze business processes and interfaces and create a big picture. The goal is a holistic approach to identify process similarities as well as interface gaps. “Speedboat” initiatives have the potential to be a good starting point to standardize processes, workflows, artifacts, and terminology. Pilot “speedboat” projects within software departments in particular have proven their worth, as they have mature working methods and holistic approaches.

The results of the standardization efforts should be a common starting point for all development departments. In order to maximize efficiencies, not every department should pursue process standardization on its own, but should instead benefit from the results of early adopters.

#6 Blunder: Use fewer tools

Over time, development environments often evolve naturally without having an underlying IT-tooling architecture strategy, which clearly defines the division of tasks, processes, and interfaces. Therefore, it is likely to have a wide range of tools with overlapping features and incoherent approaches.

Even more critical is the fact that more tools lead to more interfaces, more redundant data, more manual effort, less traceability, and less transparency. Among other things, this also means that controllability suffers, for example, overall and common reporting functions might be missing.

For companies to develop competitive and complex products while staying compliant with regulatory requirements, it is imperative to reduce the number of used tools and interfaces to a minimum. As simple as the solution may sound, the realization often fails due to different decision-makers who are responsible for the processes and tools, which do not want to give up their “realm” or change their development routines.

Solution: Unite the “realms”

To reduce the complexity and the amount of work regarding ISO 26262 and to make life with traceability easier, the number of tools should be reduced to a minimum. Often, there coexist 50+ tools in automotive development.

A reduction to 10-20 tools is possible. In praxis, this may be difficult due to different ”process & tool owners” promoting their tool or solution.

This may lead to cases, where the same process is implemented in two ways in competing tools. Top-management decision-making and a holistic deep-dive understanding seem to be the best way to solve this kind of problem.

#7 Blunder: Use appropriate tools

Quite often legacy tools are still being used due to a reluctance against implementing new tools, aligning processes, and changing habits. Using appropriate tools with, for example, state-of-the-art user interfaces, best-practice workflows, databases, and linking options makes the daily work routine much easier.

Next to the built-in abilities of the tool, preferring tools that allow the customization of workflows with regard to ISO 26262 and mandatory reviews seem to be beneficial.

The individual realization of ISO 26262 compliant system and components as well as the ever-changing regulatory compliance needs a constant adaption of workflows and required information in the tool regarding safety and ASIL classification.

Solution: Evaluate your tools and use state-of-the-art tools

Important characteristics of tools like Codebeamer or comparable tools are their flexibility to customize workflows and permissions, the possibility to create traceability and add information into fields, as well as the option of templating to scale. Next to this, they provide a solution to structure data in a systematic way and to implement or combine different agile frameworks. In case several tools are used, they also offer the option to implement individual interfaces and fitting processes.

Moreover, if used holistically, they provide a single point-of-truth database that enables the creation of traceability through all levels of the development process. Therefore, using appropriate, scalable, and more flexible tools such as Codebeamer or other comparable tools is worth the investment.

#8 Blunder: Deal with legacy data, systems and processes

Dealing with legacy systems and data is a challenge on its own in terms of compatibility with current compliance requirements. Analyzing or integrating legacy systems, workflows, and identifying relevant data is a significant problem, as the required information (e.g. interviews with former stakeholders, workflows) is often no longer available or compatible.

Safety-critical systems composed of different business processes and tools sometimes need to be manually revised and aligned with compliance regulations, which does not allow for short-term planning.

Solution: Unriddle legacy processes

In the worst-case scenario, it can take months or even years for legacy systems and processes to be completely reviewed, implemented, and compliant. Dealing with critical legacy processes requires top-level management attention, a strong leadership coalition, expert know-how, sufficient awareness/ commitment, sufficient resources, and enough time.

It is advisable to involve the developers in the change process as well to achieve higher engagement and thus a higher success rate. It is also important to find the proper balance regarding the scope and between the greenfield and brownfield approaches. This will create sufficient momentum, but also ensures that there is enough time to design the process holistically in order to gain efficiency.

About our Expert

Wolfram Bopp

Expert in the conception, development, and change management regarding tools and processes in the automotive industry, mainly in the sector of software.

Wolfram Bopp looks back on 7 years of experience in the automotive industry and ISO 26262 project experience.

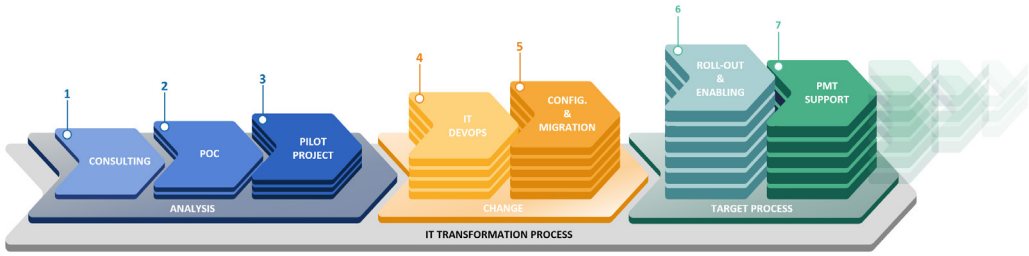
About Lösch & Partner

End-to-End IT System Integrator

In the heart of the Bavarian Silicon Valley, Lösch & Partner is a Munich-based systems engineering and IT specialist for agile and waterfall product development in the high-tech industry. Over the last 20 years, Lösch & Partner has accumulated extensive business intelligence in the field of product development. We offer solutions and services focusing on process-optimization, compliance (e.g. ISO 26262, ISO 15288, A-SPICE, CMMI), and operational support in systems engineering as well as the development, configuration, customization, and end-to-end roll-out of ALM and systems engineering tools.

The multidisciplinary team consists of technology experts, solution-oriented software developers, and process consultants, who are perfectly equipped to develop customized solutions and guarantee their efficient roll-out.

Follow Lösch & Partner on **LinkedIn**, **Xing** or **YouTube**.
Loesch.de

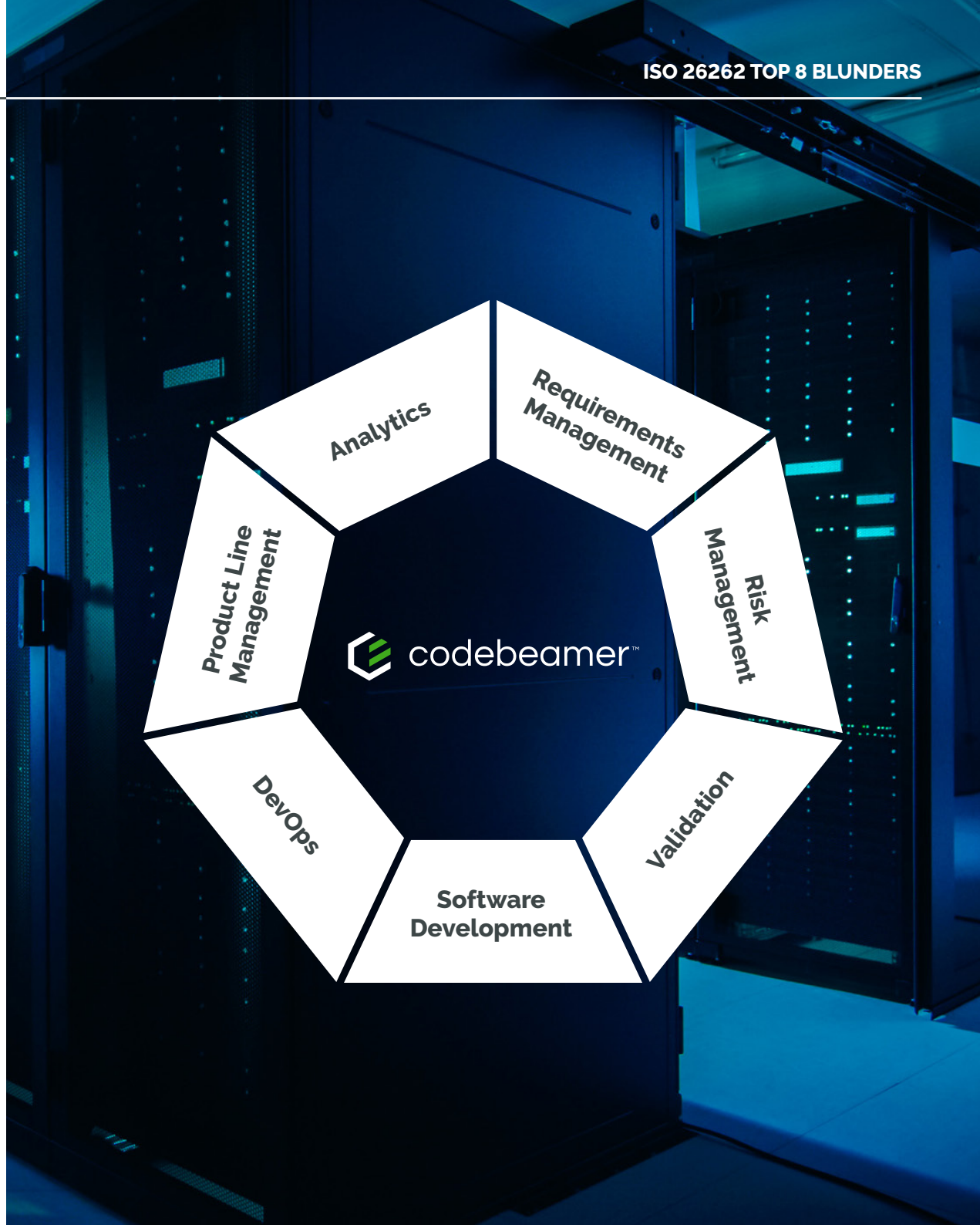


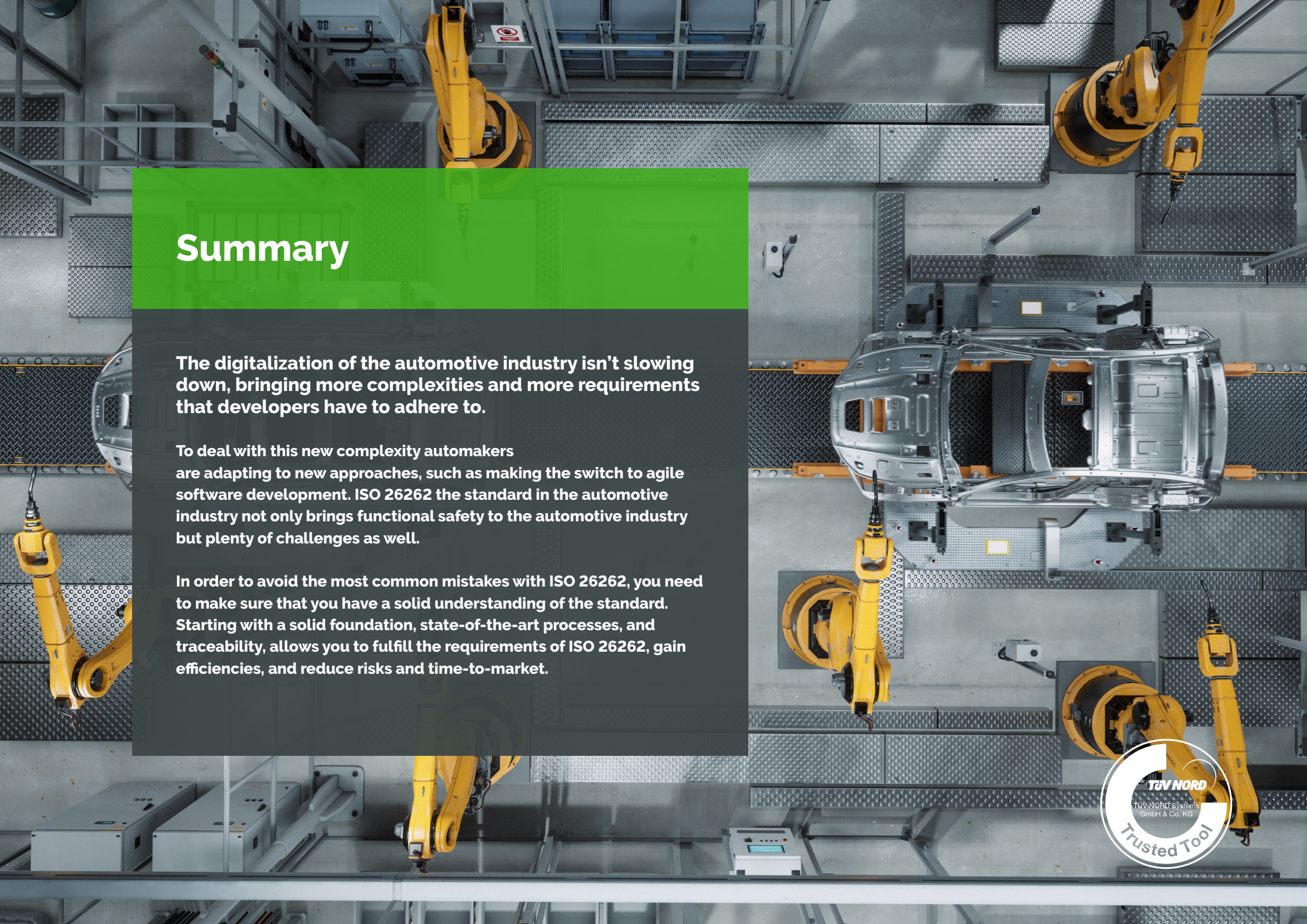
How the right Tooling can help tackle these Challenges

With various industry regulations to adhere to and a vast amount of software code, automotive development processes are probably among the most complex life cycles that companies face.

One particular part of ISO 26262 is documentation, for which you have to use adequate processes, you also need to document & report in them, show full traceability and prove process/permission control. Compliance with ISO 26262 and other standards can be simply achieved with customized Agile methods and processes.

So it all comes down to choosing the right tool for your organization. Advanced Application Lifecycle Management platforms such as **PTC's Codebeamer technology** can take the weight of documentation off your shoulders.





Summary

The digitalization of the automotive industry isn't slowing down, bringing more complexities and more requirements that developers have to adhere to.

To deal with this new complexity automakers are adapting to new approaches, such as making the switch to agile software development. ISO 26262 the standard in the automotive industry not only brings functional safety to the automotive industry but plenty of challenges as well.

In order to avoid the most common mistakes with ISO 26262, you need to make sure that you have a solid understanding of the standard. Starting with a solid foundation, state-of-the-art processes, and traceability, allows you to fulfill the requirements of ISO 26262, gain efficiencies, and reduce risks and time-to-market.

TÜV NORD
TÜV NORD Systems GmbH & Co. KG
Trusted Tool

DIGITAL TRANSFORMS PHYSICAL

121 Seaport Blvd, Boston, MA 02210 : ptc.com

005-top-8-iso-26262-blunders-02-07