

Transition to ISO 26262-6 compliant development through gap analysis



Jim Allen

29-MAR-2021

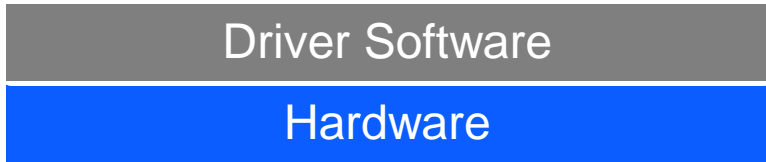
Abstract

ISO 26262 2011 First Edition has been superseded by 2018 Second Edition and both have become a base requirement for winning new business. ISO 26262 Part 2, Management of functional safety, emphasizes the importance of having a process in place to execute a Functional Safety project and to have trained staff to design product per the process. To execute a Functional Safety project it is important to quickly establish if your existing processes can be mapped to ISO 26262 or if you have to create new work flow and procedures. It is important to create the Safety Plan quickly and to conduct a conformation review so that the entire team recognizes deliverables and responsibilities. If you have never executed a ISO 26262 project it is also a good idea to contract expert advice by requesting a Gap Analysis. This formal feedback is important to drive and direct necessary resources and focus on deliverables necessary to meet the expectations of the Assessors.

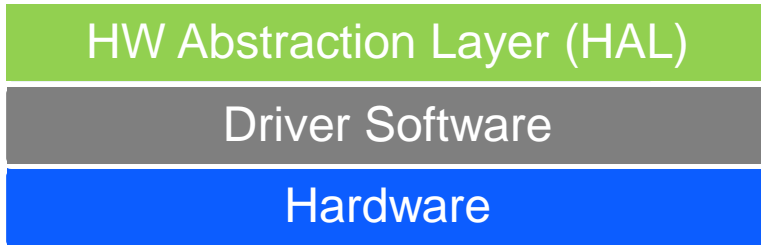
Project Background

Three project categories at BorgWarner

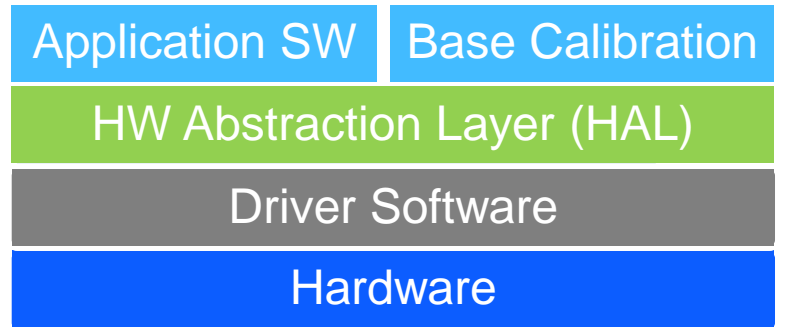
1



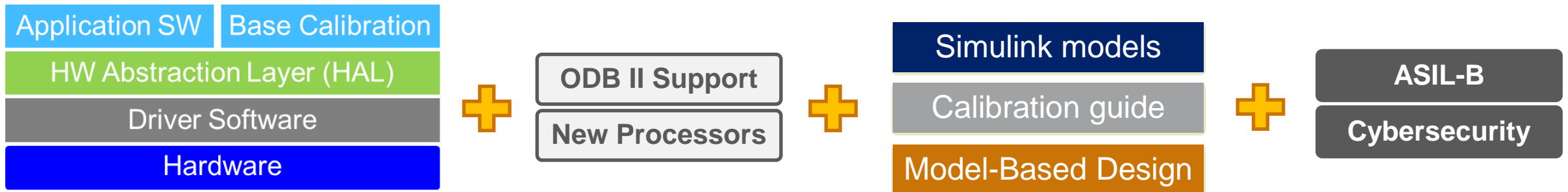
2



3



Project sharing today is based on category 3 + additional requirements



Project Starting Point



EXPERIENCE

- Company process training
- Practical product experience
- Implementing Functional Safety Req from customer
- Implementing Technical Safety Req from customer
- External training on specific tools and in areas of interest



- Upgrading development process to ISO 26262:2018
- Staffing Function Safety Engineering team
- Staffing System & Software Quality Assurance (QA) team

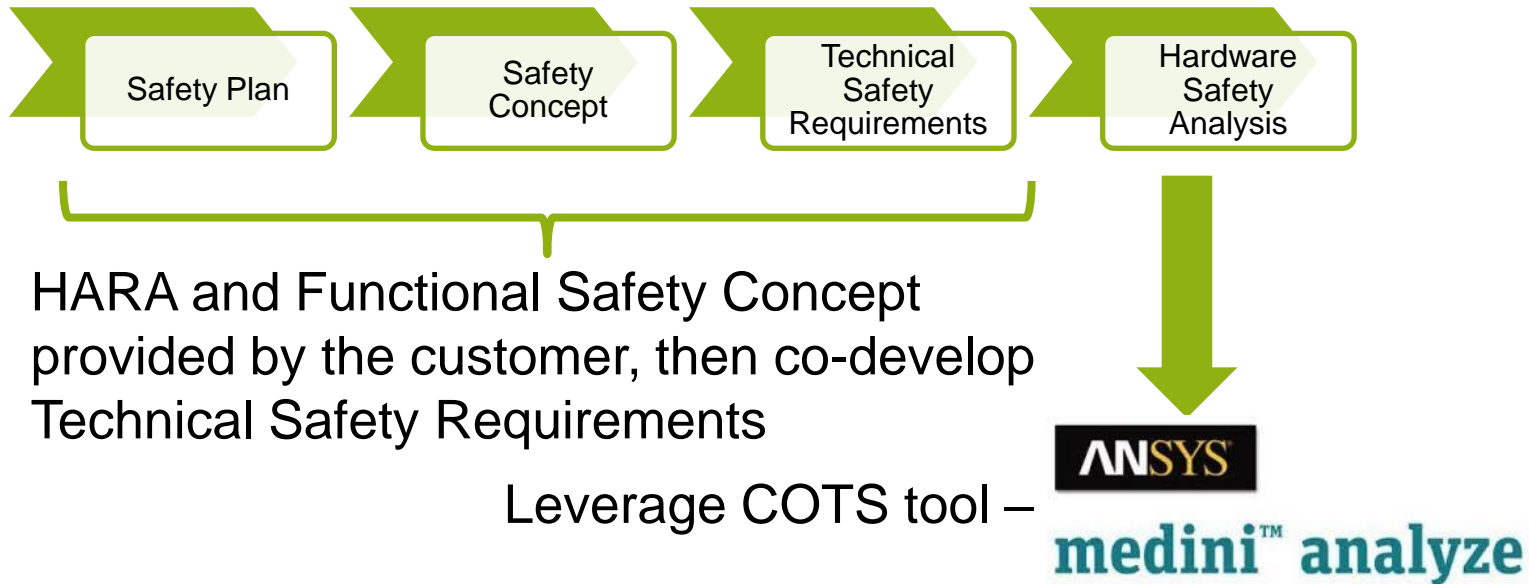
KICKOFF



- Development Interface Agreement (DIA)
- Safety Plan was delivered

The Project Mid Point

- Hardware Design
 - Provided to customer first for in vehicle testing of new software and features

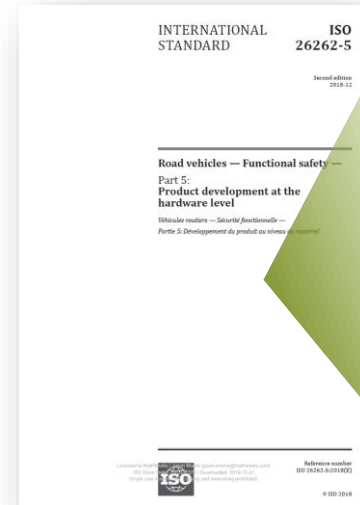


Hardware Analysis

- ISO 26262 provides detailed instruction for hardware with explicitly defined metrics and calculation methods



- This is not the case for Software requirements or ISO 26262-6
- Due to the potential of systematic failure in software
- Is our Model-Based Design development process ISO compliant?



ISO 26262-5:2018(E)

NOTE 4 When failure modes distribution and coverage of failure modes are known, $\lambda_{HWP,2}$ can be calculated as follows:

$$\lambda_{HWP,2} = \sum_{i=1}^n \lambda_i \cdot D_{FM,LSR} \cdot (1 - F_{FM,LSR}) \cdot (F_{FM,PSO} + K_{FM,LSR} \cdot (1 - F_{FM,PSO})) \cdot (1 - K_{FM,MSF}) \quad (C-6)$$

where

$\lambda_i = D_{FM,LSR}$ is the failure rate associated to i^{th} failure mode of the safety related hardware element;

$F_{FM,LSR}$ is the fraction of faults of i^{th} failure mode which are considered as safe;

$(1 - F_{FM,LSR}) \cdot F_{FM,PSO}$ is the fraction of faults of i^{th} failure mode which have the potential to directly violate the safety goal in absence of safety mechanism;

$(1 - F_{FM,LSR}) \cdot (1 - F_{FM,PSO})$ is the fraction of faults of i^{th} failure mode which are not considered as safe but which don't have the potential to directly violate the safety goal in absence of safety mechanism;

$K_{FM,LSR}$ is the failure mode coverage of i^{th} failure mode with respect to residual faults;

$K_{FM,MSF}$ is the failure mode coverage of i^{th} failure mode with respect to latent faults.

NOTE 5 For this purpose, Annex D can be used as a basis for diagnostic coverage with the claimed DC supported by a proper rationale.

NOTE 6 If the above estimates are considered too conservative, then a detailed analysis of the failure modes of the hardware element can classify each failure mode into one of the fault classes (single-point faults, residual faults, latent, detected or perceived multiple-point faults, or safe faults) with respect to the specified safety goal and determine the failure rates distributed to the failure modes. Annex D describes a flow diagram that can be used to classify the faults.

C.2 Single-point fault metric

C.2.1 This metric reflects the robustness of the item to single-point and residual faults either by coverage from safety mechanisms or by design (primarily safe faults). A high single-point fault metric implies that the proportion of single-point faults and residual faults in the hardware of the item is low.

C.2.2 This requirement applies to ASIL (B), C, and D of the safety goal. The calculation in Equation (C.7) shall be used to determine the single-point fault metric:

$$\sum_{i=1}^n (\lambda_{SP} + \lambda_{RP}) \cdot \sum_{j=1}^m (\lambda_{SP} + \lambda_{RP}) \quad (C.7)$$

Table E.1 — Safety goal 1

Component Name	Fail. rate per FIT	Safety concept to be used in the calculation of the contribution	Failure Mode	Failure Mode description	Failure mode contribution to the safety goal	Residual fault rate per FIT	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal
81	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
82	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
83	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
84	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
85	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
86	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
87	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
88	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
89	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
90	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
91	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
92	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
93	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
94	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
95	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
96	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
97	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
98	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
99	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
100	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						

Table F.4 — List of all faults or failure modes with a contribution ≥ 2 % to the overall PMHF value

Com. Name	Fail. rate per FIT	Safety concept to be used in the calculation of the contribution	Failure Mode	Failure Mode description	Failure mode contribution to the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal	Failure mode coverage of the safety goal
81	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
82	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
83	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
84	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
85	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
86	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
87	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
88	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
89	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
90	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
91	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
92	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
93	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
94	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
95	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
96	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
97	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
98	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
99	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						
100	NOTE 1	3	YES	closed	100 %	0	0.0	0.0						

The ISO 26262 Gap Analysis

Project Objectives

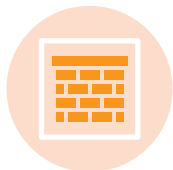


Independent evaluation prior to final Audit and Assessment



Evaluate the implemented process and ensure work products are of sufficient quality

Technical Objectives



Implementation methods for Freedom from Interference using MBD



ISO consideration between “purchased code” and “reuse code”



Efficiency improvements in using MathWorks toolchain

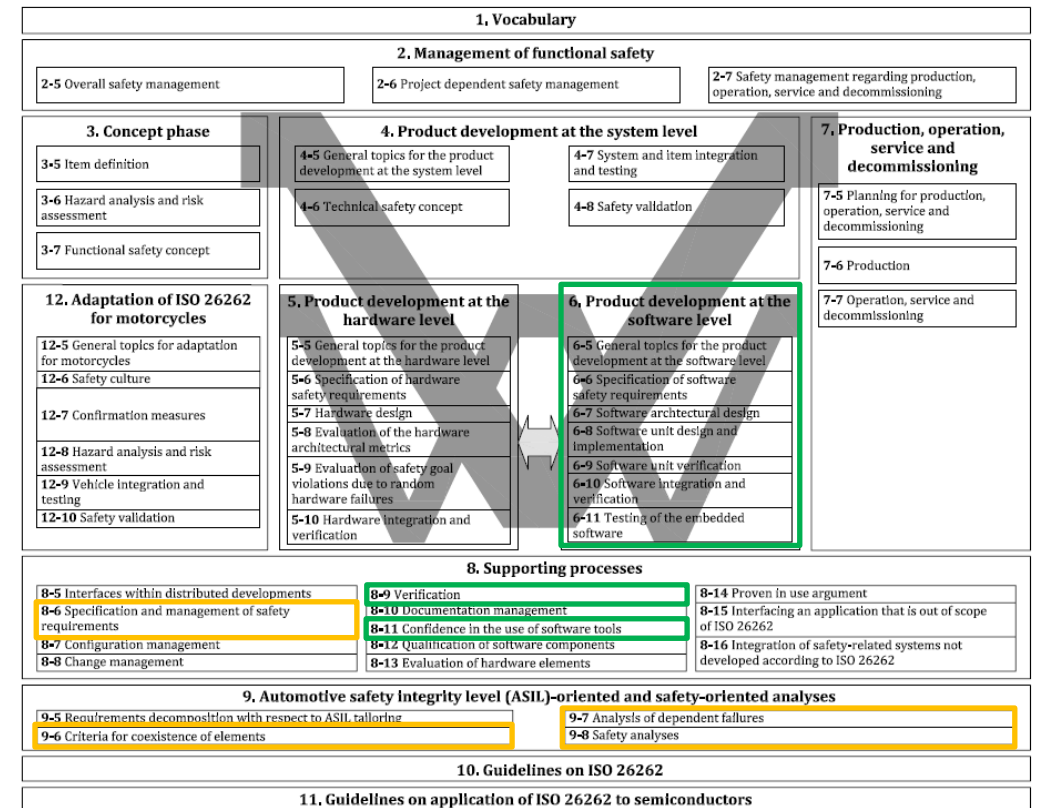


Review of Tool Qualification artifacts

The ISO 26262 Gap Analysis

- Weeklong daily interviews were held with the product development team to review their work products.
- AM – Interview and work product reviews + feedback from previous day
- PM – Analysis and review of results
- Final deliverables:
 - Gap Analysis Report
 - Examples (model/scripts)
- With the knowledge gained from the Gap Analysis Report, resources could now be directed to start the process of filling the gaps and ensuring that we would have the necessary work products for an Audit and Assessment.

- Focus area
- Peripheral area



The ISO 26262 Gap Analysis

- Weeklong daily interviews were held with the product development team to review their work products.
 - AM – Interview and work product reviews + feedback from previous day
 - PM – Analysis and review of results
- Final deliverables:
 - Gap Analysis Report
 - Examples (model/scripts)
- With the knowledge gained from the Gap Analysis Report, resources could now be directed to start the process of filling the gaps and ensuring that we would have the necessary work products for an Audit and Assessment.



Architecture



Code
Verification



Tool
Qualification

Filling the Architecture Gap

- Like many automotive projects, this project starts from a base of legacy production program.
- Most of the design were from bottom up
- Need to reconcile and ensure safety analysis is done per ISO requirement

System Engineer
(ISO 26262-4)

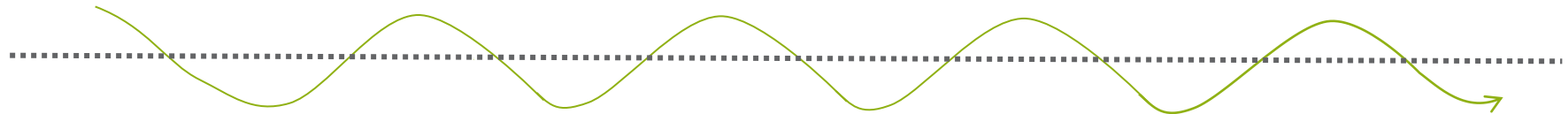


*bi-direction
tracing
Polarion "add-on"*

Two blue arrows, one pointing up and one pointing down, positioned between the text and the Polarion logo.

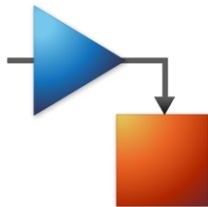
Focuses on software requirement and performing FMEA and DFA work. The results are documented, reviewed, and traced inside Polarion.

System engineering was new and was iterated with updates to software functions/features



Very practical way for executing ISO project with legacy base software

Software Engineer
(ISO 26262-6)

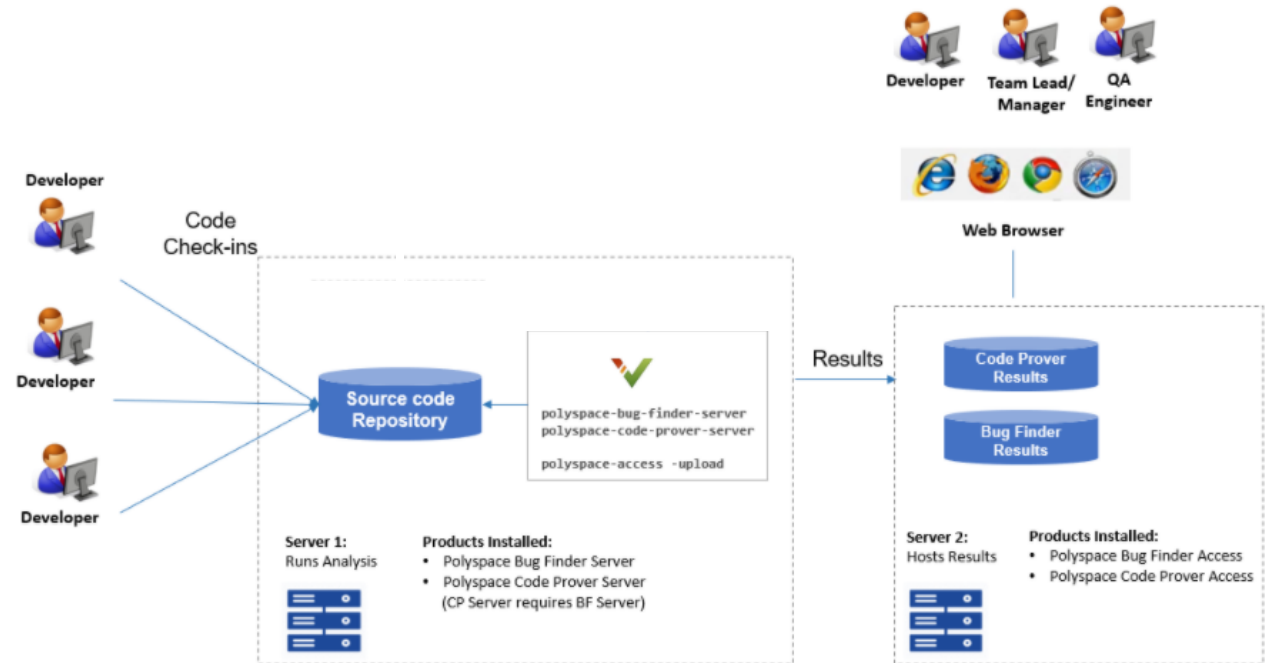


Focuses on software implementation and model verification workflow based on customer feature/functions and direction from System Engineering

Filling the Unit Test Gap (ASPICE 3.0, SWE.3 – SWE.4)

- Polyspace was used for static code analysis
 - Run-time errors
 - Coding standards (e.g., MISRA)
 - Coding metrics

- Issue: the turnaround time for Polyspace was too long for development feedback – **2 weeks** for a run



Filling the Unit Test Gap (ASPICE 3.0, SWE.3 – SWE4)

- Polyspace was used for static code analysis
 - Run-time errors
 - Coding standards (e.g., MISRA)
 - Coding metrics

- Issue: the turnaround time for Polyspace was too long for development feedback – **2 weeks** for a run



Implement recommendation configurations with MathWorks guidance



Multi-core CPU

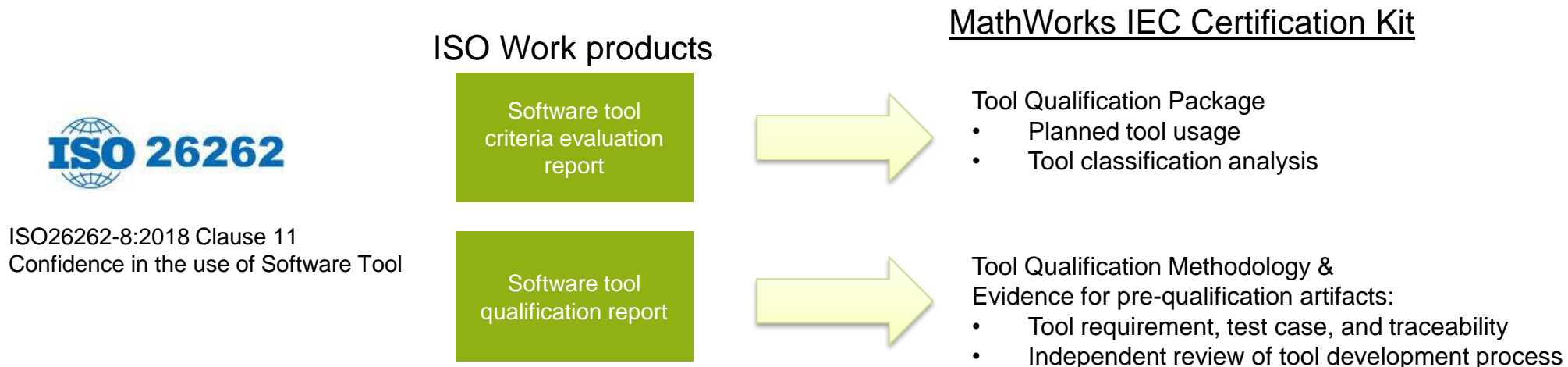
Improve Server compute power
Implement parallel processing
create batch processing



- Result
 - **Went from 2 weeks to overnight runs** provide “near real time” feedback.
 - Polyspace Access was also used for generating Web accessible report back to development team .

Filling the Gaps – Tool Qualification

- For MathWorks tools, tool qualification was done based on internal know-how from BorgWarner's technical expertise.
- For MathWorks toolchain, the results were reviewed against IEC Certification Kit as offered by supplier with similar contents.



- BorgWarner will be leveraging MathWorks Certification Kit for ISO tool qualification

Lessons learned in roles, tools, and process migration

- A Functional Safety project requires a lot of extra work that must be completed in ISO 26262-compliant fashion and on schedule to satisfy the end customer and an independent assessor.
- Sharing what we learned with other teams in the department working on Functional Safety projects created more awareness of the required processes and deliverables.
- Training classes in Functional Safety are essential for the product development teams success.
- Bring awareness to management of the role of software engineering in the architecture phase of the project and the additional work products required by a Functional Safety project.
- Sharing the advantages of using tools to automate and reduce the workload of manually creating the additional work products, for example the Polyspace automation project.
- A Gap Analysis can be a great way to assess the current situation and develop an actionable plan for moving forward. This should be considered early on during project development cycle.
- Tool qualification should be planned and performed as part of the project planning process.

ISO26262 Gap Analysis

Thank you!



Combustion



Hybrid



Electric