Agenda

- introduction
- main causes for increasing costs
- typical pitfalls
- solutions
- concluding remarks
Business Division Electronics
HELLA creates customer benefits

Comfort
- Car Access and Start Systems
- Body Electronics

A convenient environment for the passengers requires electronics as the platform to provide affordable and personalized features

Safety
- Driver Assistance functions
- Intelligent Lighting functions

Growing complexity and challenges in today’s traffic require support of electronic and lighting systems to improve traffic safety

Environment
- Energy Management
- Powertrain – Sensors & Actuators

Rising challenges concerning reduction of fuel consumption and CO₂ emissions require effective solutions

Hella is an experienced supplier of safety relevant automotive products

Energy Management

Driver Assistance Systems

Body Electronics

Sensors

Electrical Power Steering

Actuators

* typical ASIL classification
One of the main challenges: distributed development

Agenda

- introduction
- main causes for increasing costs
- typical pitfalls
- solutions
- concluding remarks
at the beginning typically too much is being done
typical behavior as the one known from the control engineering

... but are the proper things being done?

reasons for increasing costs due to implementation of functional safety in an organisation

Main reasons
- the topic Functional Safety (FS) is new for the organisation
- the experience in the domains with FS is on different levels
- acceptance is missing (introduction of FS means a change in the way of working)
- often no standard yet in the E/E development process
- too late implementation of safety in development projects
- reuse of „proven“ HW/SW solutions from the past without focus on FS
Safety management and the project organisation

- functional safety concerns all of the domains
- respective FS competence in the domains is essential

Main reasons for increasing costs with regard to available and need resources as well as FS competence

<table>
<thead>
<tr>
<th>Main reasons (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ the topic is new for the domains</td>
</tr>
<tr>
<td>■ an overview of what has additionally to be done is missing</td>
</tr>
<tr>
<td>■ there are not enough resources with respective FS competence</td>
</tr>
<tr>
<td>■ there is a need for FS training of the existing resources</td>
</tr>
<tr>
<td>➔ at the beginning expensive consultants are hired</td>
</tr>
<tr>
<td>➔ new employees have to be hired and trained</td>
</tr>
<tr>
<td>➔ existing employees have to be trained</td>
</tr>
</tbody>
</table>
Agenda

- introduction
- main causes for increasing costs
- typical pitfalls
- solutions
- concluding remarks

typical pitfalls (1/2)
### Typical Pitfalls (2/3)

- **Insufficient Safety Culture**
  - Focus on function and release
  - Missing frontloading
  - Integration of FS knowledge in the architecture not sufficient etc.
  - No awareness about impact of FS ("why is it needed?", "what is changes with regard to the status quo of the development?")

- **Insufficient Integration of FS in the Development Processes** (Missing processes, templates, guidelines etc.)

### Typical Pitfalls (3/3)

- No or insufficient safety organization (Missing resources etc.)
- No means for systematic FS cost and effort estimation
- The project team is not trained regarding FS
- Solution patterns missing or not known
- Standardized solutions missing
- No early checks ("assessments")
- Unclear escalation ways
Agenda

- introduction
- main causes for increasing costs
- typical pitfalls
- solutions
- concluding remarks

Implementation of the safety culture

Management Commitment  Standards & Processes  Continuous Improvement

SAFETY CULTURE

Integrated Safety Trainings  Safety Reporting  Monitoring  Information Exchange
improve process landscape; integrate Functional Safety

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HEER</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>HKG</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>HRO</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>TOTAL</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

| G | Low - progress according to plan, no special intervention necessary |
| Y | Medium - deviations exist, correction by means of suitable measures within the project |
| R | High - intervention by management necessary |

e.g. SPICE Level 2 as essential prerequisite for Functional Safety

example HELLA
integration of Functional Safety in the development process
establishing of a safety organisation
example HELLA

Head of Functional Safety Management

<table>
<thead>
<tr>
<th>Safety Management Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guideline and Process</td>
</tr>
<tr>
<td>Safety Experts</td>
</tr>
<tr>
<td>Safety Process Designer</td>
</tr>
</tbody>
</table>

Safety Project Management

<table>
<thead>
<tr>
<th>Project Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Manager</td>
</tr>
<tr>
<td>Safety Reviewer</td>
</tr>
</tbody>
</table>

systematic cost estimation regarding FSM

commercial domain agreement on costs

SafetyCase Taskplan — the planning tool

Work Package Planning Tool
functional safety training strategy needed

- each person involved in a safety project should get a training with focus on the domain specific tasks
- each location that develops safety relevant projects completely in own responsibility should build up own safety resources

Example HELLA:
Complete planning done by the HR for all domains

Roles concerned:
- Functional Safety Manager
- System Engineer / System Architect
- Software Architect
- Hardware Architect
- Test Manager
- ...

reusable standards – Development Interface Agreement (DIA) and System Safety Integrity (SSI) measures

- standardisation of a DIA
- creation of a DIA for customers and sub supplier from early on
- use of the DIA already in the acquisition phase

- database of SSI measures (System Safety Integrity) – e.g. RAM/ROM check, Program Flow Monitoring etc.
Reusable standards – standard solutions on macro and micro levels

**Macro level (Product lines)**

- Driver Assistance Systems
- Body Electronics
- Energy Management

**Micro level (Standard SW modules)**

Strategic decision or no decision: Obligation, responsibility and cost | R. Dorociak | Functional Safety E-EST21 | 4th International Conference „Applying ISO 26262“, Mar 25, 2014

Approach for a standardized “Variant Development” Process

Variant for AUTOSAR based Product Family Platforms

Customer Product

Reference Architecture

Component Foundation

Product Family Approach

Strategic decision or no decision: Obligation, responsibility and cost | R. Dorociak | Functional Safety E-EST21 | 4th International Conference „Applying ISO 26262“, Mar 25, 2014
early checks and escalation processes

- **cyclic checks**
  - Kick off
  - FS Assessment: "Customer"
  - FS Assessment: "Planning"
  - FS Assessment: "Development"
  - FS Assessment: "Testing"
  - FS Assessment: "Production"

- **Safety Case with report**
  - Cyclic checks on important milestones – make sure that all is done at the right time

- **escalation ways**
  - Reporting system – transparency from early on; early escalation possible

---

**Agenda**

- introduction
- main causes for increasing costs
- typical pitfalls
- solutions
- concluding remarks
concluding remarks

- main causes for increased costs
  - the topic FS is still relatively new for many organisations
  - acceptance is missing
  - too late implementation of safety
  - there is a need for FS training etc.

- typical pitfalls (missing safety culture, processes, FS cost estimation means etc.)

- solutions
  - integration of Functional Safety into the development process
  - means for systematic FS cost estimation (also for the domains)
  - training programme
  - standard solutions
  - early checks and escalation possibilities etc.

Thank you for your attention

M.Sc. Rafał Dorociak
Hella KGaA Hueck & Co.
Functional Safety E-EST 21
Beckumer Straße 130
59552 Lippstadt / Germany

Tel.: +49/ (0)2941/ 38-32263
E-Mail: Rafal.Dorociak@hella.com
www.hella.de