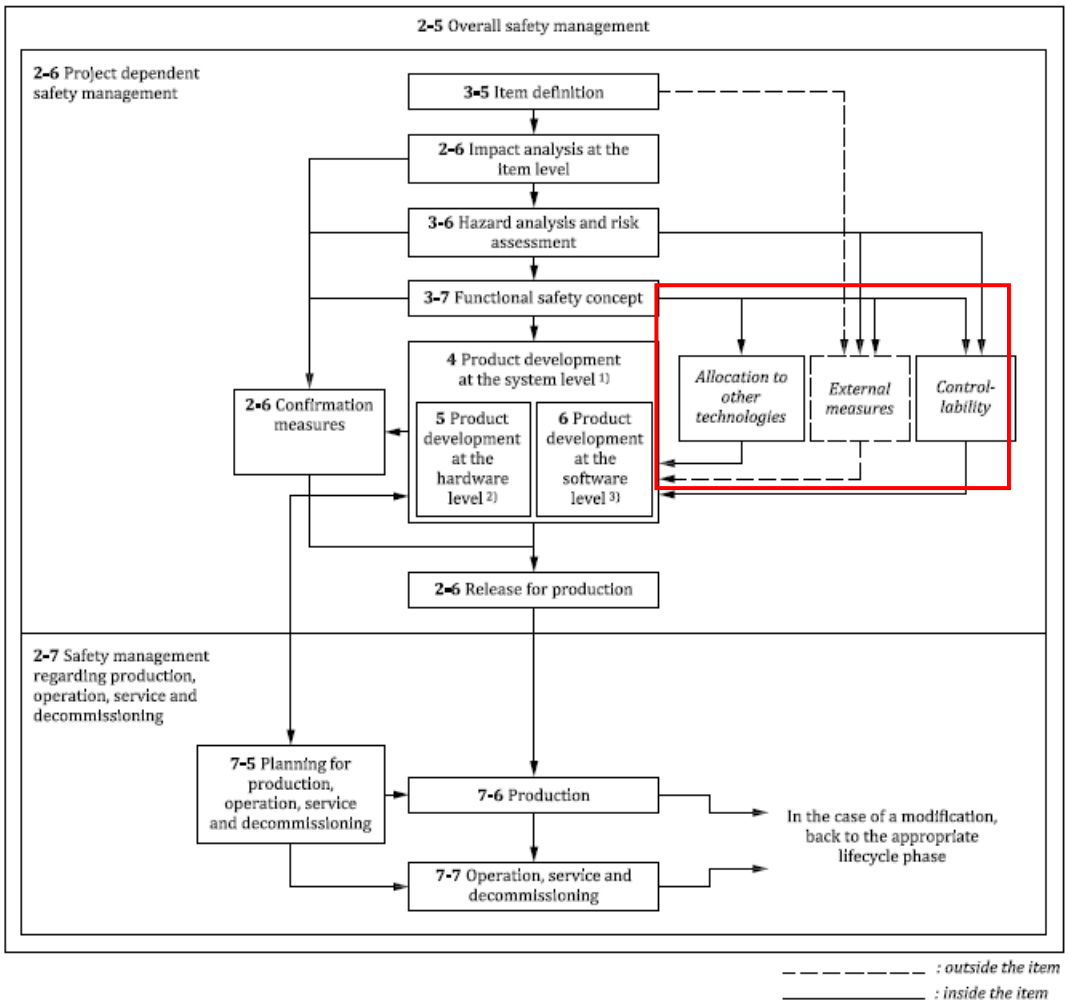
智能网联汽车写了知识分享（二）：如何进行相关项定义

安全生命周期 Safety Lifecycle

ISO26262 标准提供了一个可以定制（裁剪）的标准汽车安全生命周期（Safety Lifecycle），汽车安全生命周期涵盖了从概念设计、系统设计、软硬件开发，一直到生产、运行、服务和报废的所有活动。功能安全管理活动开始于相关项的定义。



图片来源：ISO26262-2

图 1：The Safety Lifecycle 安全生命周期

什么是相关项（Item）**、要素（Element）和组件（Component）**

相关项（Item）是在整车级实现功能的电子电气系统，

- 一个相关项至少包括一个传感器、一个控制器和一个执行器；

- 系统是一组相关联的要素（Element）；
- 要素是相关项的任何一个子级单元，可能会或不会进一步拆分成子级构成要素；
- 可以拆分的要素可以标记为系统、子系统或组件（Component）；
- 组件（Component）是一个非系统层级的，逻辑上或技术上独立的要素.

相关项的定义

相关项定义应当收集与相关项的分析和设计相关的所有信息，以支持后续功能安全活动的进行，包括

- 目的及描述;
- 功能和功能之间的关系;
- 每个功能的要求;
- 初步架构/框架;
- 其他非功能性约束条件;
- 边界或应与其他相关项/系统之间的接口;
- 法律法规要求;

在进行相关项定义时，同时应定义相关项的边界、接口以及与其和其他相关项和要素之间的交互作用的假设，考虑:

- 相关项的要素;
- 相关项行为对其他相关项或要素的效果的影响，即相关项的环境;
- 相关项与其他相关项或要素之间的交互作用;
- 对其他相关项、要素和环境所要求的功能;
- 来自其他相关项、要素和环境的功能要求;
- 相关系统之间的功能使用及分配分发至要素

- 影响相关项功能的运行情景

SEooC 的相关项定义

SEooC （Safety Element out of Context）是指无相关环境的安全要素，也就是在其开发是相关项还不存在的要素。典型的 SEooC 有标准件、通用的组件等，如一种为某些发动机管理系统(EMS)应用而开发的硬件 ECU(发动机控制单元) （适用于低端、中高端车辆)、一种实现 ECU 监控功能并确保在严重失效的情况下切断重要执行器的 ASIC（专用集成电路)、为 ECU 提供引擎同步的模块等。SEooC 的开发涉及到对产品开发的相关阶段的前置条件进行假设。通常，假设的需求的正确实现是在 SEooC 开发期间进行验证，但是其安全确认则在相关项开发期间发生。

相关项定义的工具

相关项的定义是 Fusa（功能安全）管理活动的第一步，为了准确定义相关项，需要使用适当的工具与方法，常用的方法有：

- ✓ 边界框图
- ✓ Is/Is not（是/否）分析
- ✓ 功能/要求分析
- ✓ P 图
- ✓ 接触面矩阵
- ✓ 功能矩阵
- ✓ 通讯和接口分析

相关项定义活动的工作成果（Work Product）为《相关项定义说明书》