17 Dependability

17.1 Overview

Dependability of a system is the system's ability to ensure service failures are at a level of frequency and severity that is acceptable. Dependability includes several aspects, namely Availability, Reliability, Safety, Integrity and Maintainability. The Dependability package includes support for defining and classifying safety requirements through preliminary Hazard Analysis Risk Assessment, tracing and categorizing safety requirements according to their role in the safety life-cycle, formalizing safety requirements using safety constraints, formalizing and assessing fault propagation through error models, and organizing evidence of safety in a Safety Case.

The support for safety is designed to support the automotive standard for Functional Safety, ISO/DIS 26262.

FunctionalSafetyConcept Functional Safety Concept

FunctionPort -

FunctionPrototype -

FunctionType -

Ground Indirect: Used to provide a ground in a Safety Case

HardwareComponentPrototype -

HardwareComponentType -

HardwarePin -

HazardHazard

HazardousEvent HazardousEvent

Identifiable -

InternalFaultPrototype Indirect: Used to declare internal faults of components of the Error Model.

Item Item

LifecycleStageKind Indirect: Used to define the lifecycle stage of a particular safety case.

Mode Used to represent Operating Mode including Safe State,

OperationalSituation OperationalSituation

ProcessFaultPrototype Indirect: Used to represent process faults in components of an error model. This allows declaration of required development rigor in terms of ASIL through a safety constraint.

QuantitativeSafetyConstraint Used to define Failure Rate

Rationale Indirect: Used to declare Rationale in a safety case

Requirement Used to represent Functional, technical, hardware and software requirements

RequirementsContainer Used to organize requirements in a structure

RequirementsRelationship Used to relate between requirements

SafetyCase Indirect: The safety case can be used to organize the ISO26262 related information showing that the system is safe.

SafetyConstraint Used to define the ASIL level on a particular fault or failure

SafetyGoal Safety Goal

SeverityClassKind Severity enumeration S0, S1, S2 or S3

SystemModel -

TechnicalSafetyConcept Container element for the Technical Safety Requirements allocated to architectural elements, that together form the Technical Safety Concept

TraceableSpecification -

UseCase Used in the role Operational Situation for Hazardous event

Warrant Indirect: Represents warrant in a safety case

VehicleFeature A set of Vehicle Features, realized by architectural elements, makes up the Item

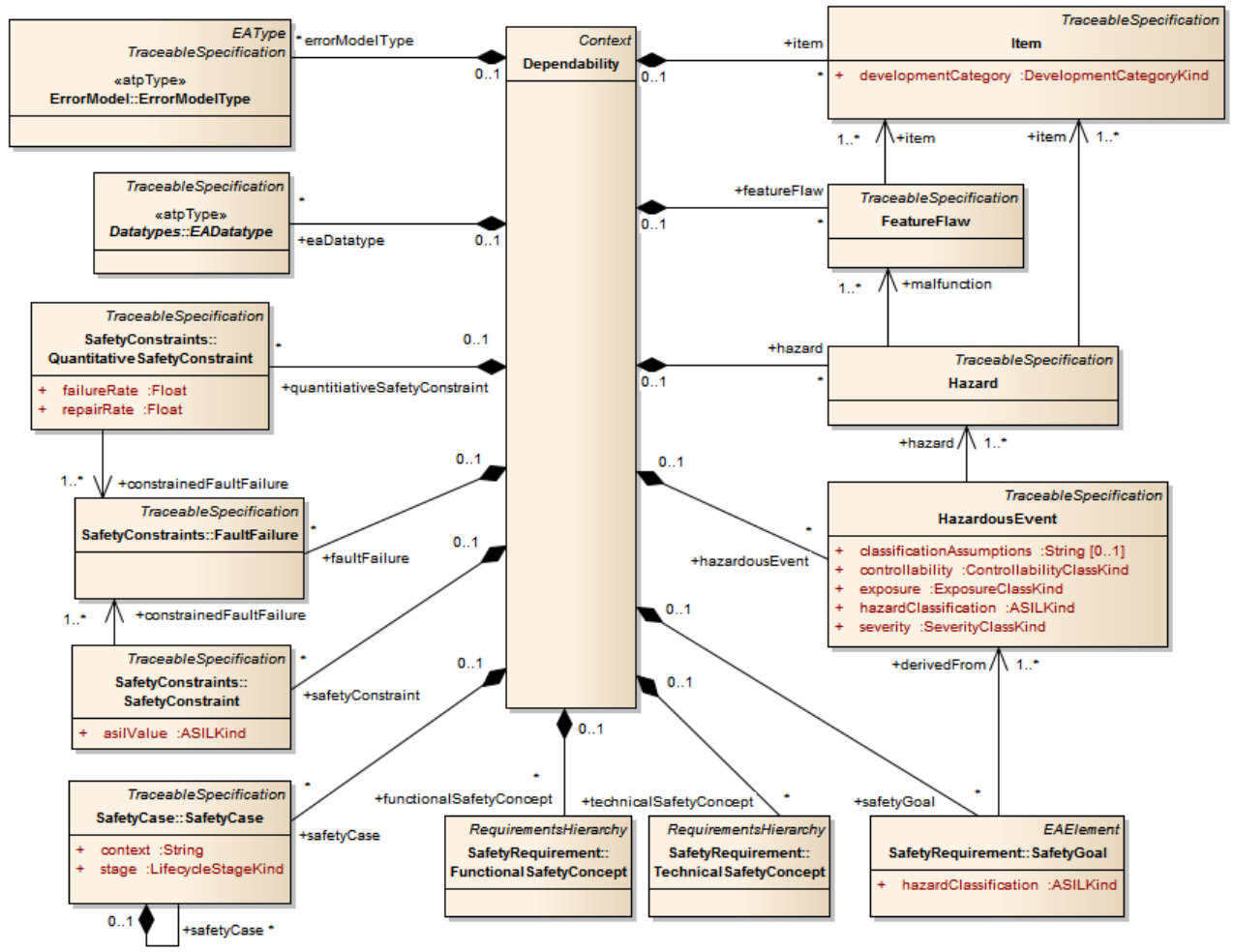

Figure 3. Diagram for organization of dependability related information.

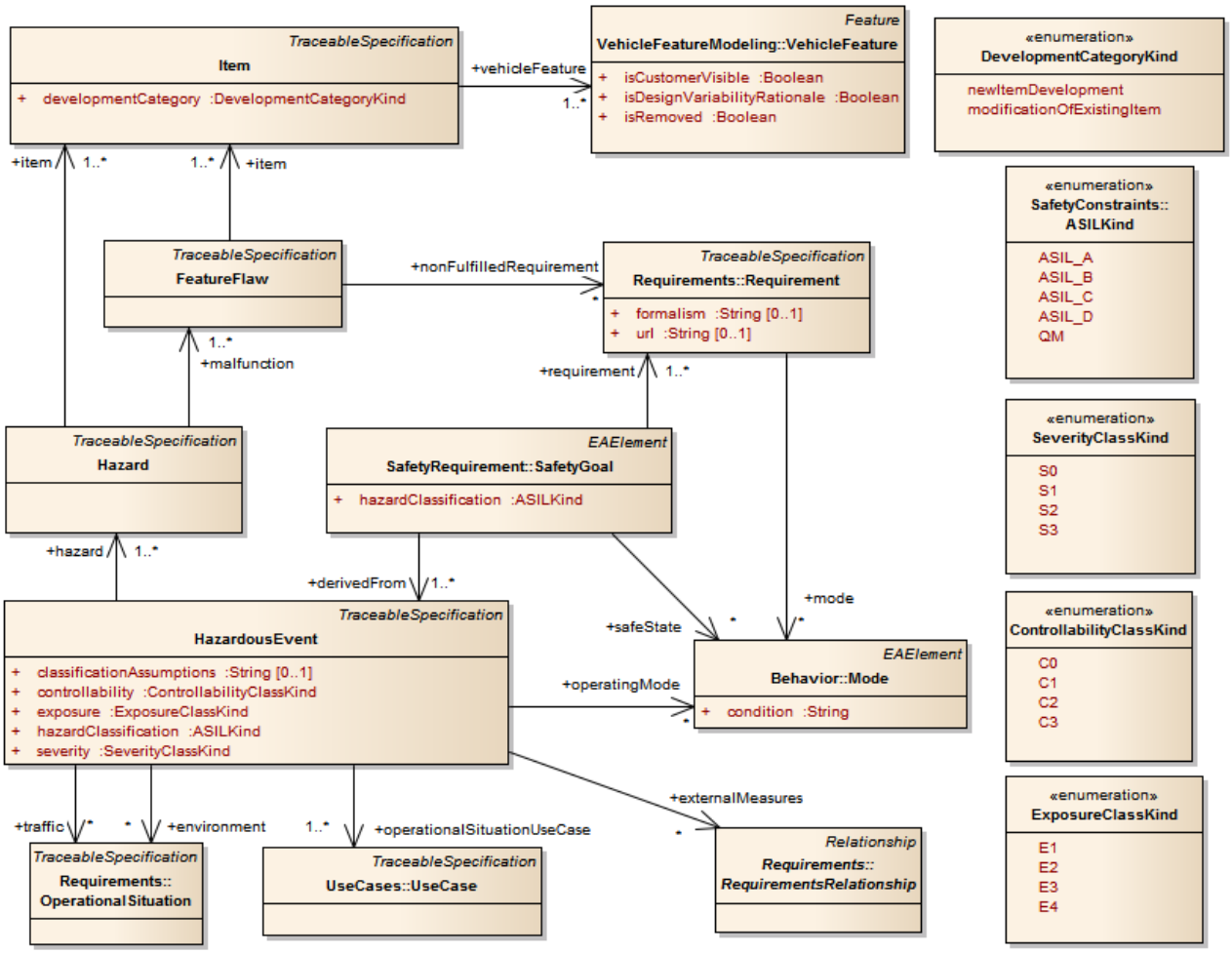

Figure 3. Diagram for Dependability.

17.2 Element Descriptions

17.2.1 ControllabilityClassKind (from Dependability) «enumeration»

Generalizations
None

Description
The ControllabilityClassKind is an enumeration metaclass with enumeration literals indicating controllability attributes C0, C1, C2 or C3 in accordance with ISO26262.

Enumeration Literals

- C0

  Controllable in general.

- C1

  Simply controllable.

- C2

Normally controllable.

- C3

  Difficult to control or uncontrollable.

Associations
No additional associations

Constraints
No additional constraints

Semantics
The semantics are defined at each enumeration literal and fully defined in the ISO26262 standard.

17.2.2 Dependability (from Dependability)

Generalizations
- Context (from Elements)

Description
The collection of dependability related information. This includes safety requirements, safety cases, safety constraints, and error modeling. This collection can be used across the EAST-ADL abstraction levels.

Attributes
No additional attributes

Associations
- technicalSafetyConcept : TechnicalSafetyConcept [*] {composite}
- eaDatatype : EADatatype [*] {composite}

  Datatypes defined in this context.
- safetyCase : SafetyCase [*] {composite}
- quantitiativeSafetyConstraint : QuantitativeSafetyConstraint [*] {composite}
- hazard : Hazard [*] {composite}
- functionalSafetyConcept : FunctionalSafetyConcept [*] {composite}
- faultFailure : FaultFailure [*] {composite}
- errorModelType : ErrorModelType [*] {composite}
- featureFlaw : FeatureFlaw [*] {composite}
- item : Item [*] {composite}
- safetyGoal : SafetyGoal [*] {composite}
- safetyConstraint : SafetyConstraint [*] {composite}
- hazardousEvent : HazardousEvent [*] {composite}

Constraints
No additional constraints

Semantics
Dependability is a container element that collects elements related to dependability. It is possible to have several Dependability elements to organize related dependability information in dedicated containers.

17.2.3 DevelopmentCategoryKind (from Dependability) «enumeration»

Generalizations
None

Description
DevelopmentCategoryKind is an enumeration with enumeration literals indicating whether the item is a modification of an existing item or if it is a new development.

Enumeration Literals

- modificationOfExistingItem

  In case of a modification the relevant lifecycle sub-phases and activities shall be determined.

- newItemDevelopment

  In case of a new development, the entire lifecycle shall be passed through.

Associations
No additional associations

Constraints
No additional constraints

Semantics
The semantics are defined at each enumeration literal and fully defined in the ISO26262 standard.

17.2.4 ExposureClassKind (from Dependability) «enumeration»

Generalizations
None

Description
The ExposureClassKind is an enumeration metaclass with enumeration literals indicating the probability attributes E1, E2, E3 or E4 in accordance with ISO26262.

Enumeration Literals

- E1

  Rare events. Situations that occur less often than once a year for the great majority of drivers

- E2

  Sometimes. Situations that occur a few times a year for the great majority of drivers

- E3

  Quite often. Situations that occur once a month or more often for an average driver

- E4

  Often. All situations that occur during almost every drive on average

Associations
No additional associations

Constraints
No additional constraints

Semantics
The semantics are defined at each enumeration literal and fully defined in the ISO26262 standard.

17.2.5 FeatureFlaw (from Dependability)

Generalizations
- TraceableSpecification (from Elements)

Description
FeatureFlaw denotes an abstract failure of a set of items, i.e. an inability to fulfill one or several of its requirements.

Attributes
No additional attributes

Associations
- nonFulfilledRequirement : Requirement [*]

  Identifies the requirements that are not fulfilled.
- item : Item [1..*]

  The item(s) for which the FeatureFlaw is identified.

Constraints
No additional constraints

Semantics
FeatureFlaw represents functional anomalies derivable from each foreseeable source, nonFulfilledRequirements identifies those requirements that correspond to the FeatureFlaw.

17.2.6 Hazard (from Dependability)

Generalizations
- TraceableSpecification (from Elements)

Description
The Hazard metaclass represents a condition or state in the system that may contribute to accidents. The Hazard is caused by malfunctioning behavior of E/E safety-related systems including interaction of these systems.

The Hazard does not address hazards such as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behavior of safety related electrical/electronic systems.

Attributes
No additional attributes

Associations
- item : Item [1..*]

  The item for which the Hazard is identified.
- malfunction : FeatureFlaw [1..*]

  The deviation of the item's operation compared to specified behavior.

Constraints
No additional constraints

Semantics
The Hazard element represents a condition or state in the system that may contribute to accidents. The associated malfunction identifies the FeatureFlaw that corresponds to the Hazard.

17.2.7 HazardousEvent (from Dependability)

Generalizations

- TraceableSpecification (from Elements)

Description

The HazardousEvent metaclass represents a combination of a Hazard and a specific situation, the latter being characterized by operating mode and operational situation in terms of a particular use case, environment and traffic.

Attributes

- classificationAssumptions : String [0..1]

  The classificationAssumptions attribute denotes assumptions concerning the classification of the Hazard.

- controllability : ControllabilityClassKind [1]

  The controllability by the driver or other traffic participants defined by the enumeration C0, C1, C2 or C3 in accordance with ISO26262.

- exposure : ExposureClassKind [1]

  The probability of exposure of the operational situations defined by the probability attributes E1, E2, E3 or E4 in accordance with ISO26262.

- hazardClassification : ASILKind [1]

  The ASIL-Level shall be determined for each hazardous event using the estimation parameters in accordance with ISO26262.

- severity : SeverityClassKind [1]

  The severity of potential harm defined by the severity attributes S0, S1, S2 or S3 in accordance with ISO26262.

Associations

- operatingMode : Mode [*]

  OperatingMode denotes the Operating mode of the item.

- externalMeasures : RequirementsRelationship [*]

- traffic : OperationalSituation [*]

  A definition of the traffic situation in terms of adjacent vehicles, pedestrians and other dynamic aspects. Represents the external and dynamic aspects of the vehicle operating situation.

- environment : OperationalSituation [*]

  A definition of the road environment in terms of road conditions, lanes, geometry, etc. Represents the external and static aspects of the vehicle operating situation.

- operationalSituationUseCase : UseCase [1..*]

  Operational situation with respect to the activities of actors, typically the driver.

- hazard : Hazard [1..*]

  The Hazard that together with the operational situation constitutes the HazardousEvent.

Constraints

No additional constraints

Semantics
The HazardousEvent denotes a combination of a Hazard and an operational situation. The controllability and severity attributes shall be consistent with the operational situation and operational scenario, and the Exposure shall reflect the likelihood of the operational situation and scenario.

17.2.8 Item (from Dependability)

Generalizations
- TraceableSpecification (from Elements)

Description
The Item entity identifies the scope of safety information and the safety assessment, i.e. the part of the system onto which the ISO26262 related information applies. Safety analyses are carried out on the basis of an item definition and the safety concepts are derived from it.

Attributes
- developmentCategory : DevelopmentCategoryKind [1]

  The Item entity identifies the scope of safety information and the safety assessment, i.e. the part of the system onto which the ISO26262 related information applies. Safety analyses are carried out on the basis of an item definition and the safety concepts are derived from it.

Associations
- vehicleFeature : VehicleFeature [1..*]

Constraints
No additional constraints

Semantics
Item represents the scope of safety information and the safety assessment through its reference to one or several Features.

17.2.9 SeverityClassKind (from Dependability) «enumeration»

Generalizations
None

Description
The SeverityClassKind is an enumeration metaclass with enumeration literals indicating the severity attributes S0, S1, S2 or S3 in accordance with ISO26262.

Enumeration Literals
- S0

  No injuries.
- S1

  Light and moderate injuries.
- S2

  Severe and life-threatening injuries (survival probable).
- S3

  Life-threatening injuries (survival uncertain), fatal injuries.

Associations
No additional associations

Constraints
No additional constraints

Semantics
The semantics are defined at each enumeration literal and fully defined in the ISO26262 standard.