Research Data B: Text-based Definition of the BSafeML Profile

The following tables provide a text-based alternative to the UML profile diagram in Figure 5 in the paper. The tables do not define any features of BSafeML that are not already shown in the profile diagram.

| **SafeML::hazard** | | |
| --- | --- | --- |
| **Inherits from** | **Description** | |
| SysML::Block | An inherent hazard | |
| **Tagged value** | **Type** | **Description** |
| Type | Enumeration, SafeML::Hazard\_type = { Radiological, Chemotoxic, Fire/explosion, Mechanical, External } | The nature of the energy associated with the hazard |
| **Relationship** | **Target** | **Description** |
| UML::Dependency | UML::UseCase, UML::Actor, UML::Activity, SysML::Block | The system elements or interfaces that give rise to the hazard |
| SafeML::hazard\_realization | SafeML::harm | The potential consequence of the hazard being realized |

Table B1: The modified SafeML Hazard stereotype.

| **SafeML::harm** | | |
| --- | --- | --- |
| **Inherits from** | **Description** | |
| SysML::Block | A qualitative consequence of a hazard being realized | |
| **Relationship** | **Target** | **Description** |
| SafeML::hazard\_realization | SafeML::hazard | The inherent hazard that may result in the harm |

Table B2: The modified SafeML Harm stereotype.

| **SafeML::hazard\_realization** | | |
| --- | --- | --- |
| **Inherits from** | **Description** | |
| SysML::AssociationBlock | The condition through which an inherent hazard is associated with an actual consequence; corresponds to the centre of a bow-tie diagram | |
| **Tagged value** | **Type** | **Description** |
| Bounding consequence | Enumeration, SafeML::Letter\_label = {A, B, C, D} | Severity of the worst credible consequence that follows from the hazard realization, on a qualitative scale |
| Frequency | Float | Frequency that the hazard realization occurs, assuming no mitigation |
| **Relationship** | **Target** | **Description** |
| UML::Dependency | UML::Activity, SysML::Block | The system element that makes it possible for the hazard to be realized |
| SafeML::risk\_reduction | BSafeML::safety\_function | Mitigations against the hazard realization |
| Owns (owned behaviour) | BSafeML::fault\_sequence | Sequences of events that cause the hazard realization |
| SafeML::hazard\_realization defines the relationship between SafeML::hazard and SafeML::harm | | |

Table B3: The modified SafeML HarmContext stereotype.

| **SafeML::risk\_reduction** | | |
| --- | --- | --- |
| **Inherits from** | **Description** | |
| SysML::AssociationBlock | The reduction in consequence or frequency to be provided by a mitigation | |
| **Tagged value** | **Type** | **Description** |
| Consequence reduction | Integer | The number of levels on the qualitative consequence scale (A, B, C, D) by which the consequence is reduced |
| Frequency reduction | Float | The factor by which the hazard realization frequency is reduced |
| **Relationship** | **Target** | **Description** |
| SafeML::risk\_reduction defines the relationship between SafeML::hazard\_realization and BSafeML::safety\_function | | |

Table B4: The modified SafeML DefenceResult stereotype.

| **BSafeML::safety\_function** | | |
| --- | --- | --- |
| **Extends** | **Description** | |
| UML::Activity | Required system behaviour that either prevents a hazard realization from occurring, reduces the frequency of its occurrence, or reduces the severity of its consequences | |
| **Tagged value** | **Type** | **Description** |
| Safety function category | Enumeration, SafeML::Letter\_label = {A, B, C, D} | Represents the importance of the safety function to a safety case for operation of the system-of-interest |
| **Relationship** | **Target** | **Description** |
| SafeML::risk\_reduction | SafeML::hazard\_realization | The hazard realization against which the safety function is a mitigation |
| UML::PartAssocation | BSafeML::safety\_function | Decomposition of safety functions into a hierarchy of sub-functions |
| BSafeML::safety\_signal | BSafeML::safety\_function, UML::Action, UML::ActivityParameterNode | Another function that generates the input to or depends on the output from the safety function |
| UML::ControlFlow | BSafeML::safety\_function, UML::Action | Another function that acts in some order with respect to the safety function |
| UML::ActivityPartition | SysML::Block | The safety measure to which the safety function is allocated |

Table B5: The BSafeML SafetyFunction stereotype.

| **BSafeML::safety\_signal** | |
| --- | --- |
| **Extends** | **Description** |
| UML::ObjectFlow | A safety critical input or output passing to or from a safety function |
| **Connector target** | **Description** |
| BSafeML::safety\_function | A safety function that generates or depends on the safety signal |
| UML::Action | A system behaviour that generates an output on which a safety function depends |
| UML::ActivityParameterNode | An input or output of the overall activity to which the safety function contributes |

Table B6: The BSafeML SafetySignal stereotype.

| **BSafeML::fault\_sequence** | | |
| --- | --- | --- |
| **Extends** | **Description** | |
| UML::Interaction | A sequence of events that results in the realization of a hazard | |
| **Relationship** | **Target** | **Description** |
| Owned by (owned behaviour) | SafeML::hazard\_realization | The resultant hazard realization |

Table B7: The BSafeML FaultSequence stereotype.

| **BSafeML::incorrect\_function** | |
| --- | --- |
| **Extends** | **Description** |
| UML::Message | An error of commission: a message, instruction or invocation that leads to the realization of a hazard |
| **Connector target** | **Description** |
| UML::Lifeline | The event sequence of an element of, or interface to, the system-of-interest |

Table B8: The BSafeML IncorrectFunction stereotype.

| **BSafeML::loss\_of\_function** | | |
| --- | --- | --- |
| **Extends** | **Description** | |
| UML::MessageEndpoint | An error of omission: a missing invocation of a safety critical function | |
| **Relationship** | **Target** | **Description** |
| UML::Message | UML::Lifeline | The system element from which the message should have originated |

Table B9: The BSafeML LossOfFunction stereotype.