# Definitions

**Definition 1** (Attack Chain Multi-Stage Attack)**.** *Is the classic, tactical sequence of steps an attacker takes to compromise a single target or domain. A cross-domain multi-stage attack is a more complex and strategic campaign where the attacker's activities span multiple, distinct domains. The attack chain is not confined to one environment; instead, the attacker "crosses" security boundaries to achieve a larger goal, using one domain as a stepping stone to compromise another (e.g., infotainment → Ethernet → CAN bus). We model the attack progression as a directed acyclic graph (DAG) where vertices represent security events and edges denote potential causal relationships. An attack chain is a specific path within this DAG that traces from an initial compromise to a final malicious outcome.*

**Definition 2** (Homologation and Type Approval)**.** *Homologation is the formal regulatory process of certifying that a vehicle system complies with international standards (UN R155, ISO/SAE 21434). Type approval is the official recognition by regulatory authorities that a vehicle model is authorized for sale and use in a specific market. These processes mandate strict adherence to safety and cybersecurity requirements, including fixed network architectures and certified software components. Any modification to certified systems, such as adding packet marking or altering gateway behavior, would require prohibitively expensive recertification, making traditional traceback methods infeasible in production vehicles. Our approach operates entirely within these certification boundaries by leveraging existing intrusion detection alerts without modifying communication stacks or certified components.*

**Definition 3** (Four Plausibility Checks)**.** *An edge between two events is admitted to the attack graph only if it satisfies all four constraints:*

1. ***Topological Check:*** *Verifies that a physical communication path exists between the source and target components. This prevents impossible paths, such as direct communication between disconnected systems.*
2. ***Temporal Check:*** *Enforces causal ordering and realistic timing between events. This addresses gateway arrival delays by accepting only links where timing falls within a safe budget derived from normal operations.*
3. ***Semantic Check:*** *Validates protocol and functional compatibility between consecutive events. This prevents semantically invalid sequences, such as linking unrelated operations or mismatched targets.*

4. ***Kinematic Check:*** *Ensures that physical effects implied by events are consistent with the vehicle's actual motion state (e.g., speed, brake status). This prevents chains that are technically possible but physically impossible in the real world.*

**Definition 4** (Degree Caps)**.** *Per-node degree caps limit the number of incoming or outgoing edges for any single event node in the attack graph. For a node $\mathcal{E}_i$, the out-degree is bounded by a constant $D_{out}$ and the in-degree is bounded by $D_{in}$. This constraint prevents any single event from becoming a hub for an impractically large number of potential causal connections, thereby controlling exponential path growth.*

**Definition 5** (Duplicate Suppression)**.** *Duplicate suppression merges near-identical events within a sliding time window to prevent redundant edges. If multiple events $\mathcal{E}_i, \mathcal{E}_j, \mathcal{E}_k, \ldots$ arrive within a time threshold $\Delta t_{merge}$, they are merged into a single representative event. This reduces the number of nodes in the graph and eliminates parallel edges that would otherwise be created between these duplicate events, significantly pruning the search space.*

*The four checks enforce a bounded in-degree and out-degree for each event in the sliding-window DAG. Rather than exploring an exponential path space, the reconstruction algorithm operates over a sparse graph whose size grows approximately linearly with the number of alerts in the window.*

**Definition 6** (Chain Finalization)**.** *A chain is finalized when it exits the analysis sliding window or reaches a dead end in the graph. Finalization involves:*

1. ***Pruning:*** *Removing redundant or suboptimal chains to maintain compactness.*
2. ***Evidence Trail:*** *Compiling a complete record of all per-edge validation results (topological path code, temporal residual, semantic rule ID, kinematic predicates).*
3. ***Export:*** *Serializing the finalized chain as a compact record for downstream analysis or alerting.*

**Definition 7** (Chain Pruning)**.** *Chain pruning is the process of removing redundant or suboptimal attack chains to reduce complexity and improve interpretability. Pruning criteria include:*

- ***Subsumption:*** *Removing chains that are strict subsets of longer, more complete chains.*
- ***Dead-End Elimination:*** *Discarding chains that terminate prematurely without reaching a critical security event.*
- ***Low-Evidence Filtering:*** *Removing chains supported by few weak or low-confidence edges.*