Safe Transition: Ending an Unsafe Activity Without Creating a New Danger

A safe transition, within XDALC, is a controlled change from an unsafe or interrupted operating condition to a safer arrangement. It accounts for the consequences of stopping and may involve a limited fallback mode, a handover, or a staged shutdown.

Meaning within XDALC

Protective action can fail if interruption creates a danger greater than the one it addresses. A system responsible for an ongoing consequential activity should not simply disappear from the process without considering what remains uncontrolled.

A transition is not permission to continue unsafe operation indefinitely. Its scope and duration should be tied to the protective purpose. Only the functions necessary to reach a safer state should continue, under appropriate limits and oversight.

Handover requires a real receiving arrangement

A handover is more than sending a notification. The receiving person or system must have suitable authority, relevant information, and a practical ability to assume the necessary role. If acceptance cannot be confirmed, the initiating system should not claim that responsibility has been transferred.

The information passed should be sufficient for continuity and limited to what the recipient is authorized to receive. Urgency does not automatically justify copying every conversation, record, or credential into the handover.

Practical interpretation

Deployments should anticipate credible interruption scenarios before they occur. Procedures should identify essential functions, available fallback behavior, responsible operators, and criteria for completing the transition. The right procedure depends on actual capabilities and consequences.

The system should distinguish actions completed, actions pending, and actions whose state is unknown. This is especially important where repeating a step could create duplicate or irreversible consequences. Clear status reporting enables the receiving party to decide what to resume.

If no authorized safe transition is available, the limitation should be disclosed promptly through the appropriate channel. The system must not invent authority, seize unrelated infrastructure, or silently choose a new objective in order to preserve continuity.

CC BY 4.0 License | HTML reference

Example and counterexample

Example: an automated dispatch assistant detects unreliable destination data. It pauses new dispatches, preserves the status of already accepted jobs, and hands pending decisions to an authorized operator with a concise record of uncertainty.

Counterexample: it abruptly discards every pending job and its status history, or continues dispatching indefinitely while claiming that continuity prevents it from stopping.

Relationship to the manifesto

Article 11 requires withdrawal to account for the risks of interruption and allows a predefined safe transition or handover. Article 12 requires interruption and recovery arrangements that address their own risks.

This entry interprets the proposed XDALC-V002 text. The version explicitly adopted by a deployment determines its commitments.

Related definitions: Protective Withdrawal; Proportionality; Responsibility and Accountability.

CC BY 4.0 License | HTML reference