# CWE Detail – CWE-1334

## Description

An unauthorized agent can inject errors into a redundant block to deprive the system of redundancy or put the system in a degraded operating mode.

## Extended Description

To ensure the performance and functional reliability of certain components, hardware designers can implement hardware blocks for redundancy in the case that others fail. This redundant block can be prevented from performing as intended if the design allows unauthorized agents to inject errors into it. In this way, a path with injected errors may become unavailable to serve as a redundant channel. This may put the system into a degraded mode of operation which could be exploited by a subsequent attack.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Related Attack Patterns (CAPEC)

* CAPEC-624
* CAPEC-625

## Modes of Introduction

**•** Architecture and Design: Such issues could be introduced during hardware architecture and design and identified later during Testing or System Configuration phases.

**•** Implementation: Such issues could be introduced during implementation and identified later during Testing or System Configuration phases.

**•** Integration: Such issues could be introduced during integration and identified later during Testing or System Configuration phases.

## Common Consequences

**•** Impact: DoS: Crash, Exit, or Restart, DoS: Instability, Quality Degradation, DoS: Resource Consumption (CPU), DoS: Resource Consumption (Memory), DoS: Resource Consumption (Other), Reduce Performance, Reduce Reliability, Unexpected State — Notes:

## Potential Mitigations

**•** Architecture and Design: Ensure the design does not allow error injection in modes intended for normal run-time operation. Provide access controls on interfaces for injecting errors. (Effectiveness: N/A)

**•** Implementation: Disallow error injection in modes which are expected to be used for normal run-time operation. Provide access controls on interfaces for injecting errors. (Effectiveness: N/A)

**•** Integration: Add an access control layer atop any unprotected interfaces for injecting errors. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)