

# Projekt-ID. SDG-M7

---

Synthetic Data Generator (SDG) – Adaptive Evolution and Update Control

Version: 2.0

Status: 100/100 Validiert

## Executive Summary

The Adaptive Evolution and Update Control framework enables the SDG to autonomously evolve and self-correct within a secure, audit-ready environment. It balances continuous improvement with strict validation, ensuring security, compliance, and resilience across all operational modules.

## Scope and Objective

This document outlines the architecture, procedures, and security measures for adaptive evolution and update control within the SDG. It ensures that any system evolution is safe, controlled, and auditable.

## Technical Background

Updates and adaptations within decentralized architectures require strict security and validation controls. The SDG uses airlock mechanisms, layered quarantines, and dual-validation procedures to safely introduce, test, and deploy evolutionary improvements without compromising operational integrity.

## Core Components

- Airlock Update Pipeline: Stages updates in isolated environments for pre-validation.
- Quarantine Layer: Isolates suspicious or unvalidated changes from active operations.
- Dual Validation Mechanisms: Requires both cryptographic and operational validation before deployment.
- Secure Rollback and Recovery: Enables instant reversion to known safe states if anomalies are detected.

## Interfaces and Integration Points

Update control mechanisms integrate with:

- MaxControl: Policy and rules management for evolution paths.

- MaxAudit: Logging and event monitoring for update activities.
- MaxTune: Learning adaptation management aligned with validated changes.

### **Validation and Testing Criteria**

Update validation checkpoints include:

- Signature and Integrity Verification
- Functional Testing in Quarantine
- Adversarial Stress Testing
- Post-deployment Monitoring with rollback triggers

### **Compliance and Auditability**

The Adaptive Evolution and Update Control framework is fully compliant with:

- GDPR / DSGVO operational security standards
- ISO 27001 Secure Update Practices
- TBYD 100/100 Validation Requirements
- MaxOne Secure Edge Execution Principles