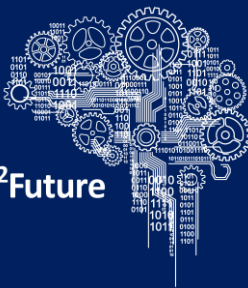


# SAFE INDUSTRIAL GENERATIVE AI

## Multi-Tier Hybrid Shielding Layer for Accelerated Compliance Verification and Safety Policy Enforcement



Faiza Mushtaq<sup>1</sup>, Amer Kajmakovic<sup>1</sup>, Amel Jelidi<sup>1</sup>  
Pro2Future GmbH<sup>1</sup>  
<sup>1</sup>Sandgasse 34, 8010 Graz



### MOTIVATION & GOALS

Black-box generative models cannot be safely deployed in manufacturing environments governed by strict standards as **ISO 12100 HARA** directive without absolute behavioral containment. This project engineered a dependable compliance verification layer that fill the gap between **probabilistic AI flexibility** and **deterministic safety enforcement**.

Project FactBox

Project Name

SafeFlow

Project ID

MFP Prod.2

Duration

48 Months

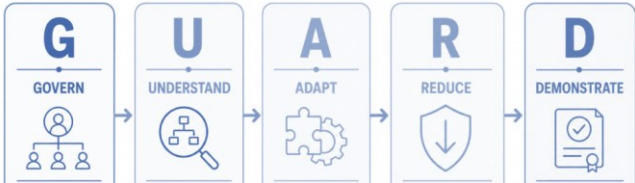
Area 4.1

Cognitive Products

Project Lead:

DI. Dr. Amer Kajmaković

### APPROACH

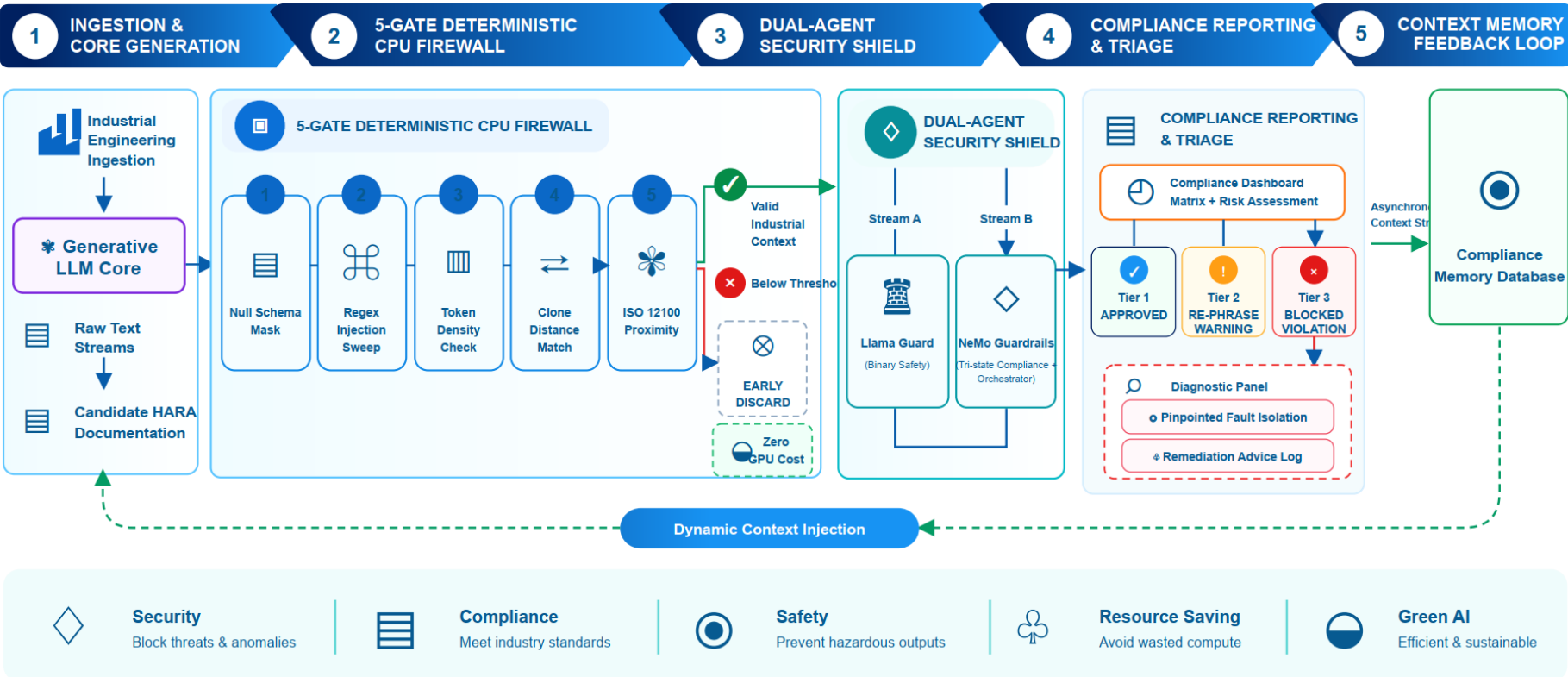


Our framework deploys a hybrid multi-stage defensive firewall to verify **strict industrial compliance** and safely isolate local edge LLM workflows, which provides a production-ready, **resource-optimized** shield tailored explicitly for edge deployment on the factory floor.

### CONTRIBUTION

- Scientific contribution
- Novel architecture for secure industrial automation pipelines.
  - Dual-engine cross-examination for standards-compliant LLM-generated engineering artifacts.
- Economic contribution
- Resource-efficient Green AI on edge hardware.
  - Reduced computation and energy use through local filtering.
  - Lower operational costs by avoiding redundant GPU processing.

### SAFETY SHIELDING SYSTEM ARCHITECTURE



Contact: Faiza Mushtaq, Pro2Future GmbH, faiza.mushtaq@pro2future.at, +43 660 6298204  
Acknowledgement: This work was supported by Pro2Future II (FFG, 911655) and Siemens.