



Advanced Production & Security

CSIR AI Symposium

24 August 2026

CSIR ICC

Dr Hildegarde Koen

Divisional AI Champion

Principal researcher, CCIS – D&S



science, technology
& innovation

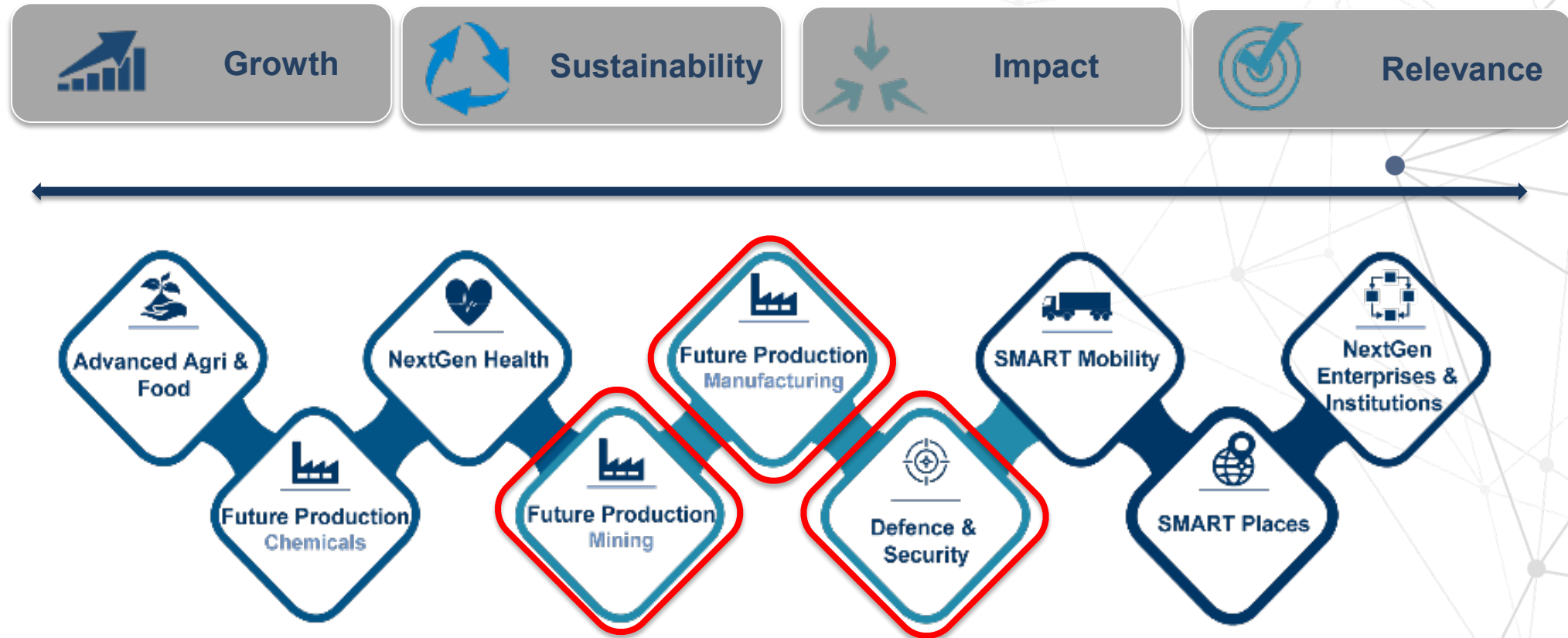
Department:
Science, Technology and Innovation
REPUBLIC OF SOUTH AFRICA



CSIR

Touching lives through innovation

The CSIR Strategic Intent and RDI Pillars





Focus is on responsible AI adoption within the division

The challenge is on balancing **innovation**, **competitiveness**, and the **protection** of sensitive information.





**The question is not
“Should we use AI?” but
rather “What can be safely
used with which data
classifications?”**

Objective: Accelerate RD&I and operational effectiveness without exposing defence, security, client, or sovereign information.



The Context

AI copilots are being embedded into Microsoft 365, IDEs, Adobe, engineering software, etcetera.

Researchers can gain significant productivity improvements through this AI assistance.

However, many AI-enabled products contain cloud-based processing components.

Sensitive information can be exposed through prompts, uploaded files, or generated outputs.



The Primary Risk – Data Leaks

Defence designs, architectures, and specifications may be exposed to external services.

Prompts may contain classified or sensitive operational details.

Cross-border data movement can create regulatory and sovereignty concerns.

Single user actions can unintentionally disclose high-value information.



Other Risks

“Shadow AI”: staff use unsanctioned AI tools when approved alternatives are unavailable.

AI supply-chain risk from changing vendors, models, and hosting arrangements.

Hallucinations and incorrect outputs in intelligence or engineering decisions.

Loss of intellectual property and proprietary CSIR knowledge.



Three Tier AI Adoption Model Needed

1

Public AI

Generic research and public information only

2

Enterprise AI

Approved corporate information and productivity use cases

3

Sovereign / Secure AI

Sensitive, defence and national-security environments



Move the AI to the data. Do not move sensitive data to the AI.

Deploy AI within trusted environments.

Classify AI systems according to information sensitivity.

Maintain human accountability for final decisions.



Strategic Opportunity for the CSIR

Become a national leader in Trusted Sovereign AI.

Develop air-gapped and on-premise LLM capabilities.

Enable secure knowledge management for government and defence.

Support strategic industries with trusted AI infrastructure.

Provide AI assurance, validation, and certification capabilities.

AI Value-Add for APS and Industry (0-18 Months)

Divisional benefits

Faster literature reviews, technology scouting, and patent analysis.

AI-assisted proposal writing, reporting, and software development.

Searchable institutional knowledge across programmes.

Faster systems engineering, verification, and test planning.

Industry Impact

Defence: Intelligence fusion, cyber security automation, multispectral ISR analytics.

Mining: Predictive maintenance, safety analytics, production optimisation.

Advanced Manufacturing: Defect detection, additive manufacturing optimisation, automated quality assurance.

Robotics: AI-assisted perception, navigation, and robotic inspection systems.



AI Value-Add for APS and Industry (18-36 Months)

Divisional benefits

AI-integrated digital twins for accelerated experimentation.

AI-augmented research and model generation.

Faster concept-to-demonstrator cycles.

Sovereign secure AI platforms for sensitive applications.

Industry Impact

Defence: AI-enabled C2, cognitive radar/EW, autonomous platforms, sensor fusion.

Mining: Autonomous operations and digital mines.

Advanced Manufacturing: Digital twin factories, real-time AM monitoring, adaptive production scheduling.

Robotics & Physical AI: Autonomous inspection, logistics, human-robot teaming.



Recommended Research Themes

Advanced Production and Security



On-premise, air-gapped & classified-environment AI systems



Multi-sensor fusion, cognitive radar/EW, AI-enabled C2, AI in space



Smart mining, manufacturing optimisation, generative design, predictive maintenance



AI on sensors, vehicles, drones, and disconnected environments



Quality, systems verification, and validation



Autonomous robots, intelligent sensors, perception, navigation, and human-robot collaboration

Defence and Security Impact Areas



Aerospace Systems



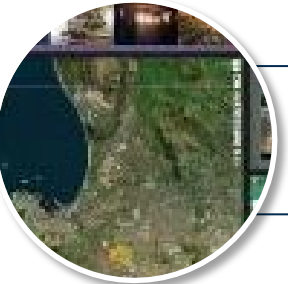
**Radar and
Electronic Warfare**



Optronics Sensor Systems



Landward Sciences



**Command, Control and
Integrative Systems**



**Technology for
Special Operations**



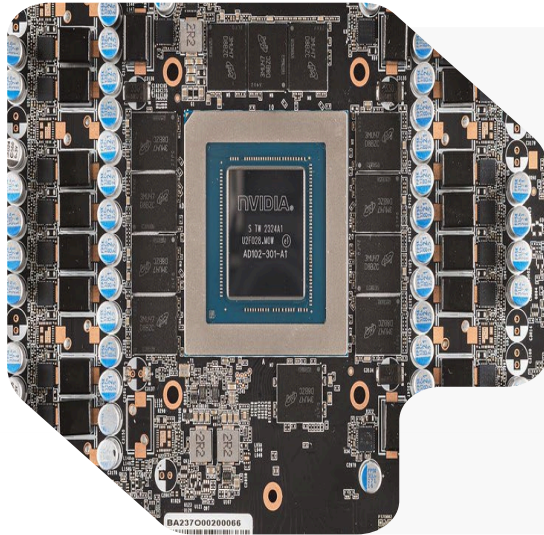
**Information and Cybersecurity
Centre**

Use Case Examples: Aerospace Systems Impact Area



Legacy software migration

As part of a larger obsolescence programme at the CSIR wind tunnels, LLMs are utilised to back-annotate legacy Fortran code to modern coding languages so that hardware upgrades can be implemented



Air-gapped LLM capability
Pilot-scale setup of a network secure and isolated dedicated compute node

DO-178 Standards Compliance

Automated testing and real-time standards verification for safety-critical airborne software



Wind Tunnel Rig Tracking

A future project to use convolutional neural networks (CNNs) to optically track wind tunnel model position and attitude

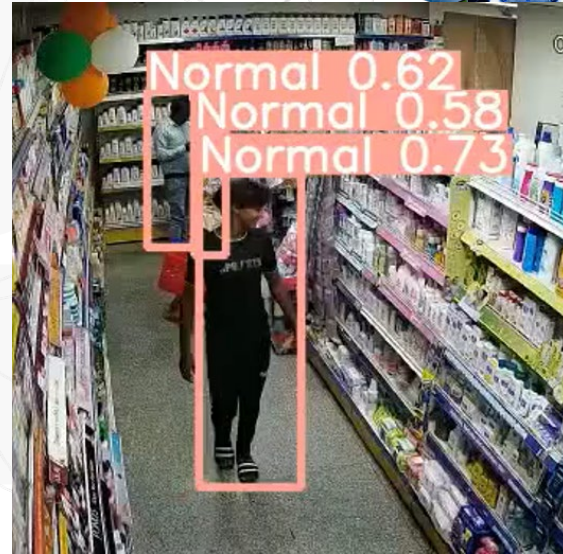


Use Case Examples: CCIS Impact Area



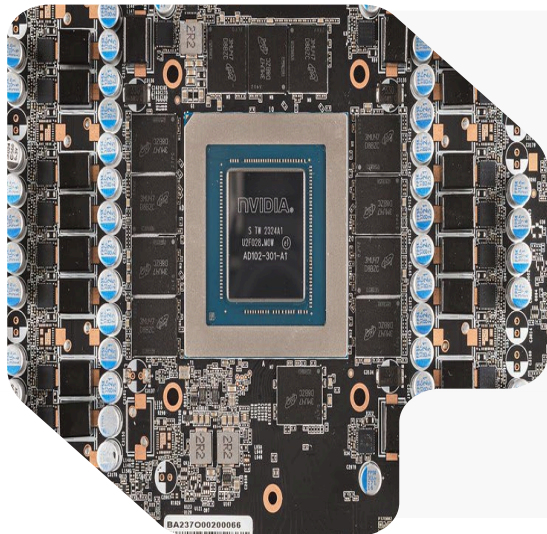
Drone Detection and Classification Platform

Using trained machine learning models to detect and classify drones according to make and model using RF signals.



Video AI Capability

Using machine learning models to detect objects, persons, faces.



Generative AI
Developing and training offline LLMs for use by the military.



AI & ML Workshops

Presenting AI & ML workshops to the DoD, SANDF, and Armscor since 2019.

Use Case Examples: Landwards Impact Area



TinyML acoustic UAV detection

On-device sound analysis for drone detection using TinyML on low-power hardware.



Radar-camera sensor fusion

AI-powered fusion of radar and vision for robust detection, classification and tracking.



ML-based gesture-controlled turret

IMU and vibration-aware AI enables intuitive, hands-free turret control.



Computer vision for target/UXO-related detection

AI models for object and anomaly detection to enhance situational awareness and safety.



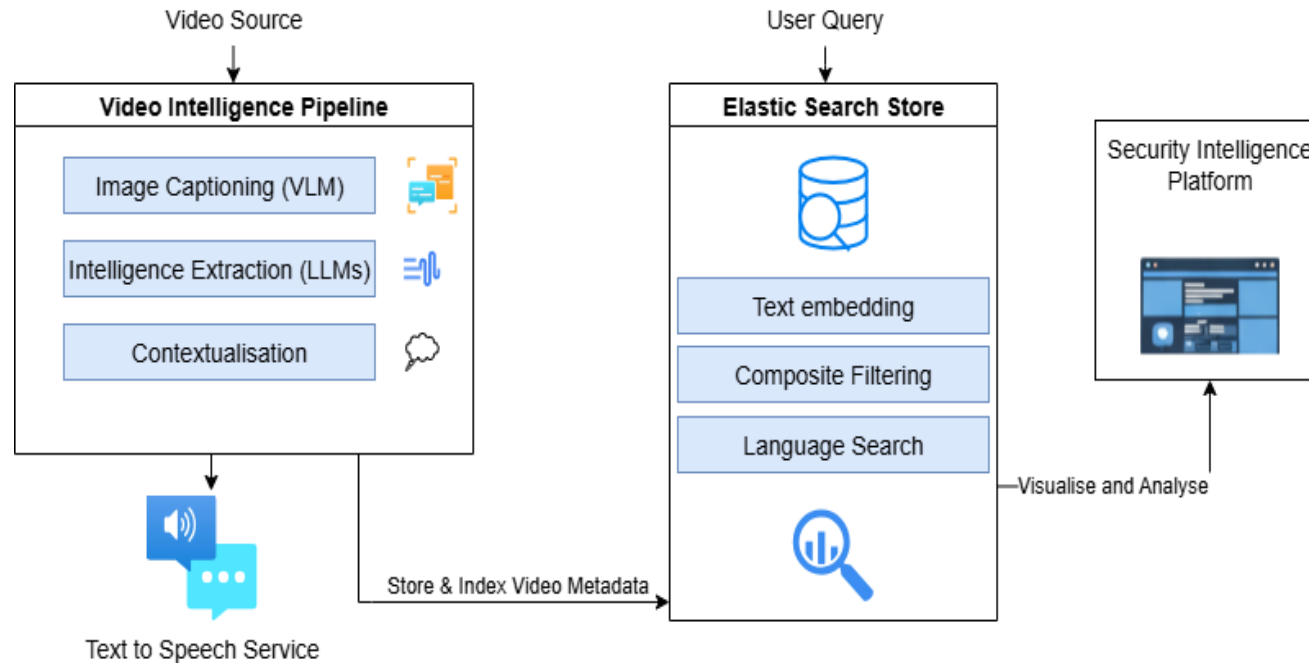
Edge-AI engineering and resource-aware deployment

Design and optimisation of AI models for embedded platforms with strict power, memory, and latency constraints.



Sensors → AI inference → Actionable insights

Use Case Examples: OSS Impact Area



Intelligent Video Analytics (IVA) Platform

Image processing algorithms using CNNs for object detection and tracking, action recognition.

Development of:

Advanced AI that understands images better
Narrates scenes, identifies objects, backgrounds, and predicts actions.

Multi-camera tracking which allows for moving object tracking and identification over multiple camera locations.

Emerging Opportunities

- **Multi-modal edge AI**
 - Fuse radar, camera, audio, environmental and communications data for richer understanding at the edge.
 - Fuse satellite data, weather data, flight data for richer C2 and situational awareness on the ground.
- **Adaptive/context-aware AI**
 - AI that adapts to terrain, platform dynamics, and mission context for improved reliability and performance.
- **Noise-robust and open-set recognition**
 - Develop AI that performs in noisy, real-world conditions and can handle novel or unknown objects.
- **AI-enabled/adaptive tactical communications**
 - Intelligent, adaptive mesh networking with AI-driven link management and spectrum optimisation.
- **Trusted and deployable AI**
 - Explainable, secure and safety-assured AI systems ready for deployment in harsh operational environments.



Thank you