GRECTA

Product safety compliance infrastructure

REGULATING A DUAL-USE COUNTER-DRONE SYSTEM

Case study: AutoFly AI Robotics SIA and the Sky Control System

REGULATORY ASSESSMENT, REMEDIATION BACKLOG AND CUSTOM FRAMEWORKS

GRECTA REGULATORY RESEARCH · NOVEMBER 2026

Publisher	Grecta Regulatory Research
Date	November 2026
Client	AutoFly AI Robotics SIA (Latvia), Sky Control System. Founder and chief executive: Deniss Isakovs
Status	Draft for client approval. Case study and regulatory analysis. Not legal advice.

Contents

Summary 3

Chapter 1. The client and the product 4

Chapter 2. The regulatory perimeter 5

Chapter 3. The engagement 6

Chapter 4. The custom frameworks 7

Annex. Instruments referred to 8

About Grecta 9

Summary

1. Sky Control is a counter-unmanned aircraft system (counter-UAS) developed by AutoFly AI Robotics SIA, a company established in Latvia. The system detects drones through sensor fusion and radio-frequency detection, supports the intercept decision with an AI decision engine, and neutralises the target by net-based interception. Its founder and chief executive is Deniss Isakovs.

2. Grecta carried out a regulatory assessment of the product, converted the findings into a remediation backlog, and is building custom frameworks for the regimes that reach it and that no standard framework covers.

3. **The central finding.** A counter-UAS product sits at the boundary between defence and civil product law. Whether the AI Act applies depends on the intended purpose of the system as supplied. Article 2(3) of Regulation (EU) 2024/1689 excludes AI systems placed on the market, put into service or used exclusively for military, defence or national security purposes. A system sold to airports, prisons and energy operators does not fall inside that exclusion. A system sold only to armed forces does. The same product can therefore sit on either side of the line, and the line is drawn by how it is offered, documented and contracted.

4. That finding fixed the structure of the work. The assessment recorded the intended purpose for each customer segment, the backlog was written against the regimes that apply to the civil and dual-use configuration, and the custom frameworks were built for regimes that general compliance platforms do not model for this product category.

Chapter 1

The client and the product

1. **The company.** AutoFly AI Robotics SIA is a Latvian company. It is organised around a hardware and defence entity and a separate AI software entity. The counter-UAS product is marketed as the Sky Control System. It was previously presented under the LUMEN platform name and the customer-facing name has since changed. Documents issued before the change use the earlier name.

2. **The product.** The system combines several sensing modes, including radio-frequency detection, into one picture of the airspace. An AI decision engine classifies a detected drone and supports the choice of response. The response is a net-based interception, which is a non-lethal means of neutralising the target.

3. **The customers.** The product is positioned for critical infrastructure and airport security as well as defence buyers. The positioning is dual-use, and the regulatory consequences of that choice are set out in Chapter 2.

4. **Relationship to Grecta.** The founder of Grecta has a separate advisory relationship with AutoFly AI Robotics SIA. This case study is published with that relationship disclosed, and the findings should be read with it in mind.

Chapter 2

The regulatory perimeter

1. The regulatory perimeter of a dual-use counter-UAS product is not set by the technology. It is set by the intended purpose declared for each configuration and customer segment. Five questions determine it.

(a) **Is the AI system excluded under Article 2(3) of the AI Act?** The exclusion applies only where the system is used exclusively for military, defence or national security purposes. Civil or dual-use supply removes the exclusion for that configuration.

(b) **If it is in scope, is the decision engine a high-risk system?** The answer depends on whether the intended purpose falls within a use case listed in Annex III, and on whether the system is a safety component of a product within Annex I. This is decided per configuration.

(c) **Is the product a product with digital elements under the Cyber Resilience Act?** The Act sets cybersecurity requirements for such products and carves out products developed exclusively for national security or military purposes.

(d) **Does the radio-frequency equipment fall under the Radio Equipment Directive?** Any equipment that emits or receives radio waves for the purpose of radio communication or radiodetermination needs its status checked before it is placed on the market.

(e) **Does export require authorisation?** Items that can be used for both civil and military purposes are subject to licensing under the EU dual-use regime, which affects how the product can be offered to buyers outside the Union.

7. Each question has a different owner inside the company and a different evidence requirement. The assessment treated them together, because the answer to the first controls the answers to the others.

Chapter 3

The engagement

1. **Assessment.** The assessment established the intended purpose of each configuration, classified the product under each applicable regime, determined the company's role (manufacturer, provider or deployer) for each, and listed the requirements that follow with their deadlines.

2. **Backlog.** Every gap found in the assessment was written as a work item against the rule that creates it. Each item states the requirement, the evidence the company must hold, the owner and the deadline. The backlog is exported into the company's own task tracker, so remediation runs as ordinary engineering work.

3. **Custom frameworks.** Where a regime is not covered by a standard framework, Grecta builds it as a custom framework. This work is in progress. Chapter 4 describes the frameworks and their status.

Chapter 4

The custom frameworks

1. A custom framework is a machine-readable rulebook for a regime that the standard framework set does not model. It records the regime's obligations, the facts that trigger them, and the evidence that closes them, so that the same logic runs for this product as for any other.

2. The frameworks below are those the regulatory perimeter in Chapter 2 points to. They are listed with the reason each reaches the product. The status column records where each stands in the engagement.

Framework	Why it reaches the product	Status
AI Act, Article 2(3) exclusion test	Decides whether the AI decision engine is inside or outside the Act for each configuration and customer segment	To be confirmed by Grecta before release
Cyber Resilience Act	Network-connected hardware and software with digital elements, with an exclusion for exclusively military products	To be confirmed by Grecta before release
Radio Equipment Directive	Radio-frequency detection and communication equipment placed on the EU market	To be confirmed by Grecta before release
EU dual-use export regime	Licensing for items usable for both civil and military purposes	To be confirmed by Grecta before release
NIS2 (customer side)	Critical infrastructure and airport customers carry their own obligations that the supplier must be able to evidence	To be confirmed by Grecta before release

Annex

Instruments referred to

Instrument	Reference	Relevance
AI Act	Regulation (EU) 2024/1689, Article 2(3)	Exclusion for military, defence and national security systems
Digital Omnibus on AI	Regulation (EU) 2026/1744	Sets the high-risk application dates of 2 December 2027 and 2 August 2028
Cyber Resilience Act	Regulation (EU) 2024/2847	Cybersecurity requirements for products with digital elements
Radio Equipment Directive	Directive 2014/53/EU	Radio equipment placed on the EU market
Dual-use Regulation	Regulation (EU) 2021/821	Export control for dual-use items
NIS2 Directive	Directive (EU) 2022/2555	Obligations of essential and important entities

About Grecta

1. Grecta is product safety compliance infrastructure. It works out which obligations reach a specific product across every regime that applies, EU and US, and builds the infrastructure around each one: the gap list and templates to close it, tasks written against the rule that creates them, release checks, and records that update when the product or the law changes. Its coverage is cross-framework, so one product is assessed once against the AI Act, the Cyber Resilience Act, data protection, sectoral law and US regimes such as the Colorado AI Act.

2. Grecta is built by a regulatory lawyer who engaged with the European Commission during the AI Act drafting. Its deterministic logic engine is the subject of two UK patent filings.

3. To establish where a dual-use product sits across the regimes that reach it, contact yuliia@grecta.com or visit grecta.com.

ESTABLISH WHERE YOUR PRODUCT SITS ACROSS THE REGIMES THAT REACH IT

Grecta resolves every obligation that applies to a specific product across every EU and US regime that reaches it, clause by clause, turns the gaps into work your team can action, and gives the product a verification page your customers can open.

Compliance Pack pilot. Two weeks, one product, €1,500 fixed, credited in full against your first year. You receive your classification and legal role, every requirement that applies with its deadline, the gap list and templates to close it, the tasks exported into Jira or Linear, a procurement answer pack, and your product's verification page.
yuliia@grecta.com · calendly.com/yuliia-grecta/30min · grecta.com

---

Grecta Regulatory Research

Grecta is a trading name of EuroGRC OÜ, Estonia.

This document is a case study and regulatory analysis. It is not legal advice. It reflects the position at the date of publication to the best of our knowledge. EU digital law moves quickly, so the current text and your own position should be verified before relying on it.

November 2026