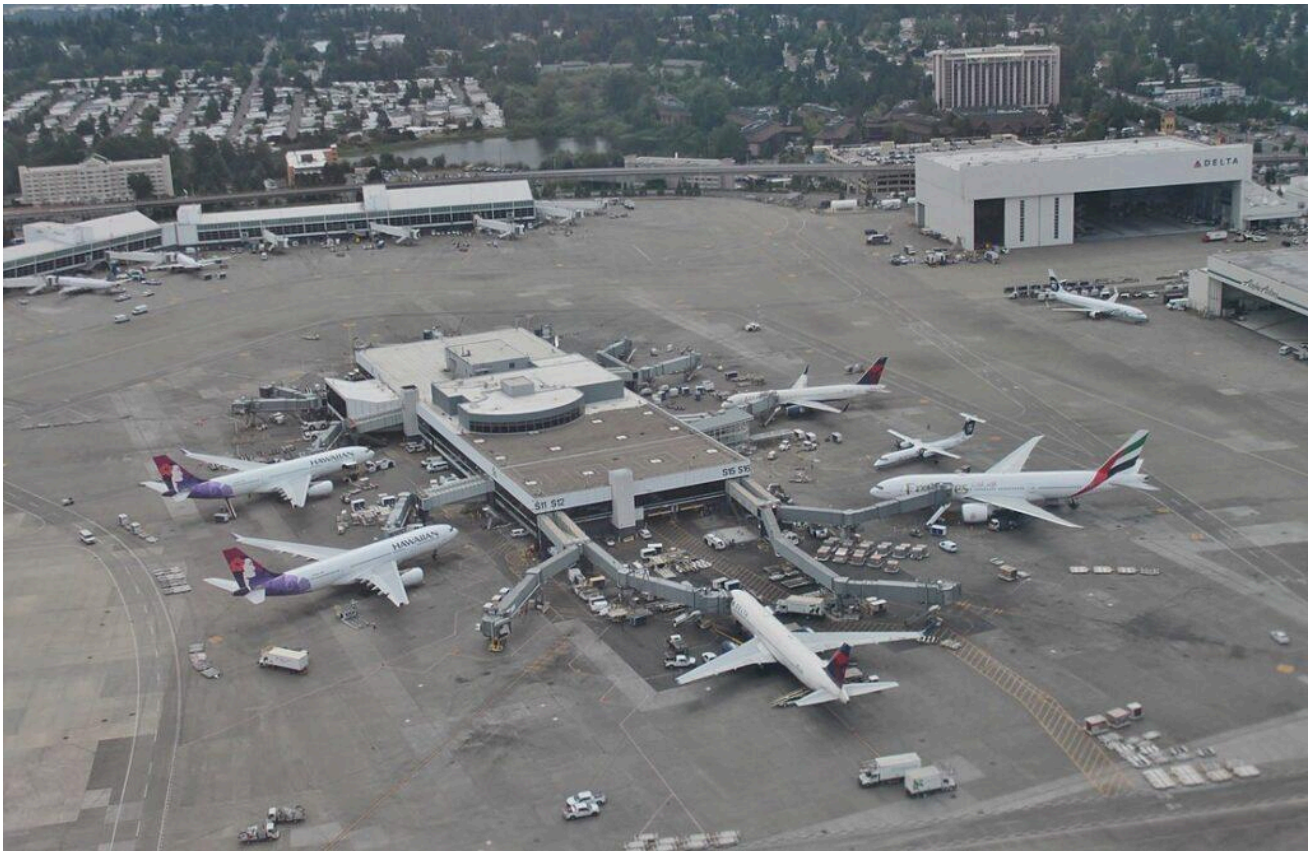
Cyberattacks on airport infrastructure are no longer limited to IT systems – even runway lighting is at risk.

Cyber Threats at Airports: Can Your Runway Lighting Hold the Line?

As airports adopt more digital and automated systems, their exposure to cyber threats grows. In fact, cyberattacks in the aviation industry surged by 131% between 2022 and 2023. While IT departments focus heavily on securing data and networks, attackers are increasingly exploring physical infrastructure as a target, especially **systems critical to aircraft operations**.

One such target is runway lighting. If a cyberattack disrupts electricity or control systems, **airfield lighting** becomes a key safety feature that must remain operational at all costs. In this scenario, when every minute matters, can your AGL keep your airport functioning?

S4GA solar runway lights operate independently from the grid and airport infrastructure.



Seattle-Tacoma Airport hit by cyberattack, 100s of flights affected. Source: aviationa2z.com.

How Centralized AGL Systems Fail

Today, airports face a wide range of cyberattacks that can disrupt critical operations. Attacks that **can directly impact AGL systems** generally fall into two main categories:

- Cyberattacks on the airfield lighting control system
- Cyberattacks on the power infrastructure

An AGL system is considered cyber-resilient when it is protected against both:

> "A cyber-resilient civil aviation system is a system that, under attack, can maintain its critical functionalities: i.e., supports safe and secure flight operations with minimal, if any, disruption."
>
> – according to the ICAO Cybersecurity Policy Guidance.

Yet in most airports today, runway lighting relies on centralized control systems and power grids, both of which are vulnerable. If hackers breach the airport's internal network, they can intercept or completely **disable the lighting control system**. In many cases, this means losing command over the entire runway lighting infrastructure.

A separate attack could target the airport's main power supply, taking out not just the lights but potentially the entire airport's operations. In either case, the consequences are immediate: the runway goes dark, flights are grounded, and the airport incurs massive operational and financial losses. This type of vulnerability was evident in the case of Mexico's OMA Group, where a ransomware attack targeted airport operations and disrupted internal systems.

In another example, Polish authorities are currently investigating whether a technical failure that paralyzed air traffic control in June 2024 may have been an act of deliberate sabotage. The outage, which disabled the PansaUTM system and halted all takeoffs for hours across the country, highlights how fragile centralized aviation systems can be—especially if cybersecurity is lacking or response protocols are not resilient enough to handle sudden disruptions.

Then, are **S4GA systems protected from the attacks** described above?

S4GA solar runway lights operate independently from the grid and airport infrastructure. Source: actenium.com.br.

S4GA: A Decentralized System With No Single Point of Failure

To respond to these threats, S4GA developed a fundamentally different system—engineered not only for performance and efficiency but also for **cybersecurity and operational independence**. S4GA airfield lighting incorporates a fully isolated network, a layered control architecture, an independent power supply in every light, and an off-grid wireless control system.

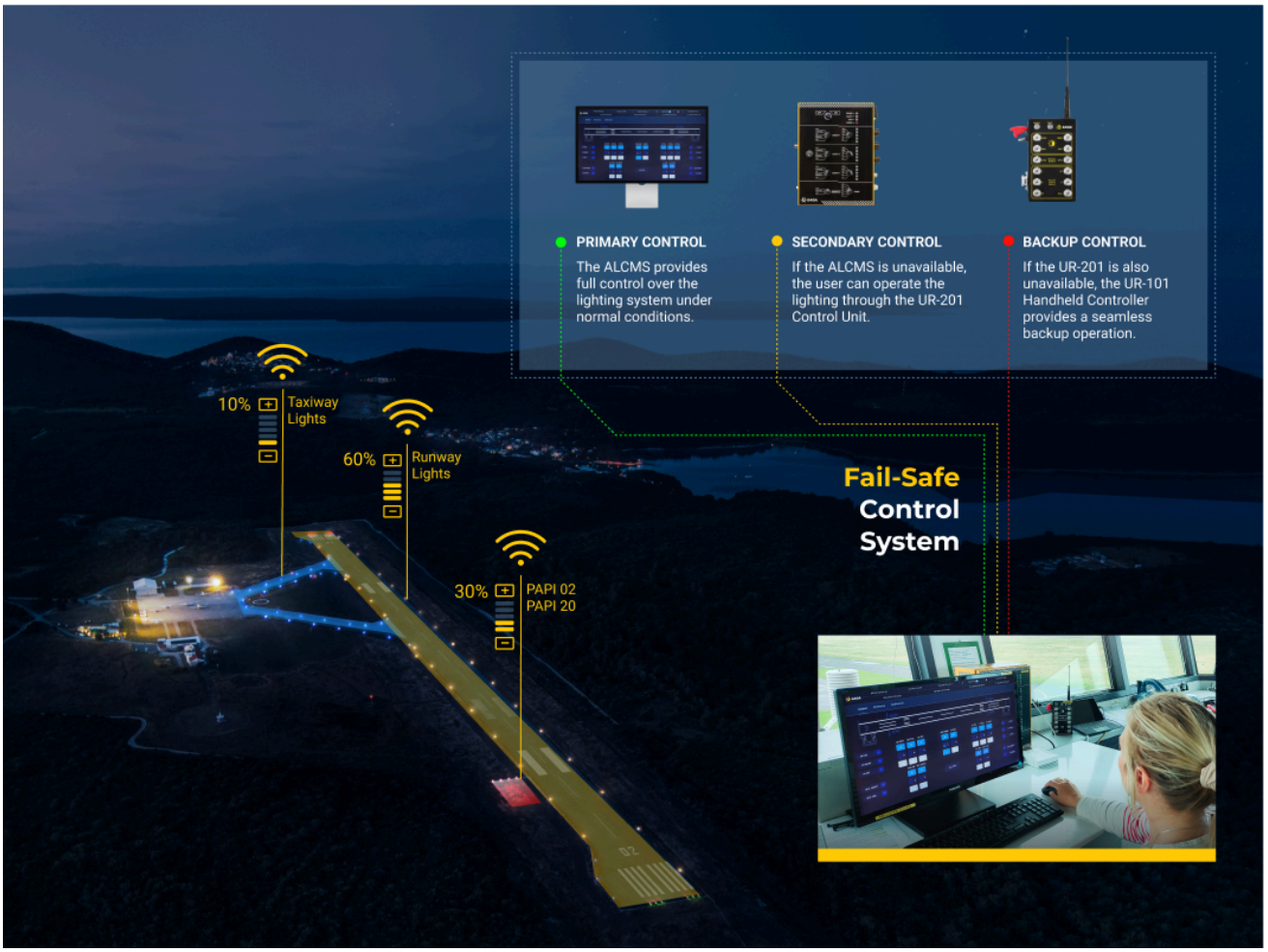
S4GA's ALCMS, resistant to warfare and secured from cyber-attacks.

Fully Isolated from Airport Networks

One of the most important features of S4GA airfield lighting is that it is completely **isolated from the airport's IT infrastructure**. The lights and the Airfield Lighting Control and Monitoring System run on a closed, secure communication loop that does not require connection to the Internet or any internal airport systems. This physical isolation offers a strong safeguard against external cyber threats attempting to penetrate through conventional network paths.

Layered Control Architecture

Instead of relying on one unit to manage the entire network, the **S4GA system uses multiple controllers**. If ALCMS — a primary control unit — is compromised, damaged, or taken offline, secondary and backup control options — UR-201 and UR-101, respectively — continue operating the airfield lighting without interruption. Emergency ON/OFF switches on each light unit also allow for quick control when a wireless network is not available whatsoever. This redundant design ensures that no single failure can bring down the system.



Safe airfield lighting operations through a multi-layered control system.

Lights with Independent Power Supply

Cyberattacks target not only AGL control systems but also the airport's broader power infrastructure. In such cases, **decentralized power sources** can make a critical difference. The S4GA system is powered just like that: each light is equipped with two independent integrated batteries. This eliminates reliance on centralized electrical infrastructure, so a power outage

at the airport has no impact on S4GA's lighting performance. This means the runway stays lit, no matter what happens to the electrical grid.

Each S4GA light includes two integrated batteries, ensuring operation even during complete power outages - no connection to the grid required.

Off-Grid Wireless Control Systems

Finally, **control is fully wireless**. It's not connected to the main power supply or CCRs—unlike conventional systems. Therefore, even if central power is lost, both lighting and control remain fully operational.

Designed to perform under the most challenging conditions, S4GA lights keep your runway operational 24/7.

S4GA: Airfield Lighting That Withstands Modern Threats

As threats evolve to target physical systems, airfield lighting must also be designed with resilience in mind. And this is how S4GA systems are designed: secured from cyber attacks and resistant to electronic warfare. Numerous airports already using S4GA airfield lighting systems no longer have to compromise between **performance, sustainability, and cybersecurity**.

These advanced protection features make it the world's safest runway lighting system, positioning S4GA as the leader in the solar airfield lighting industry.

Are you ready to protect your airport? Contact us