



EUROPEAN DRONE SUMMIT

FRANKFURT, 15/10/2018

W.J.M.R.A. van Loon

Strategic Development Director Europe



Co ESS - Acting as the voice of the security industry

Key Figures

- 25 national associations
- 24 European countries, of which 19 EU Member States
- 45,000 private security companies
- 2 million private security employees
- yearly turnover in Europe: over €40 billion.

The core values of CoESS are Quality, Safety, Compliance and Trust.

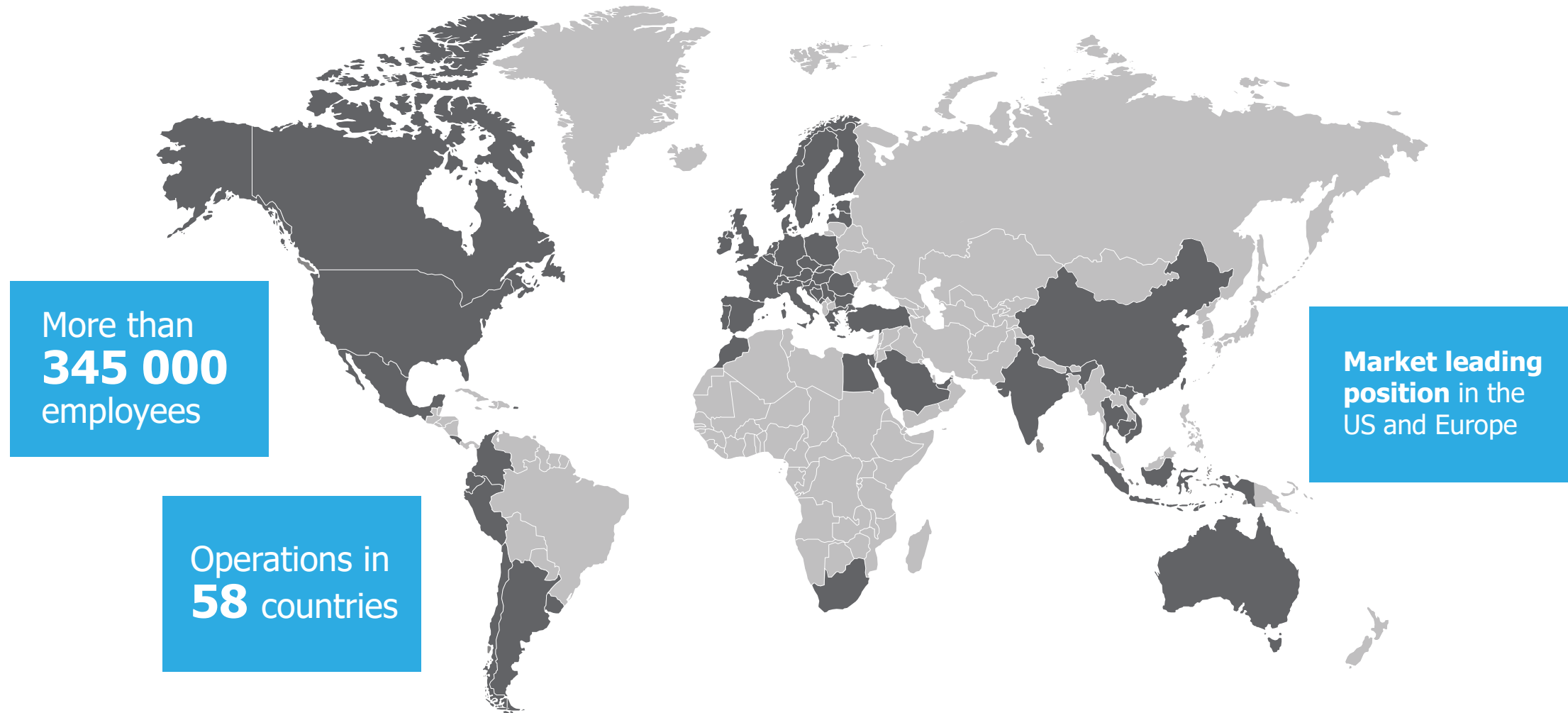
Since 2015 member of:



REGISTER OF COMMISSION EXPERT GROUPS
Expert Group on Drones (E03533)

Submission of 5 successive position papers in response to EASA and Commission publications

Securitas Group overview



Securitas

A Full Range of Protective Services



ON-SITE SERVICES



FIRE AND SAFETY



REMOTE SERVICES



ELECTRONIC SECURITY

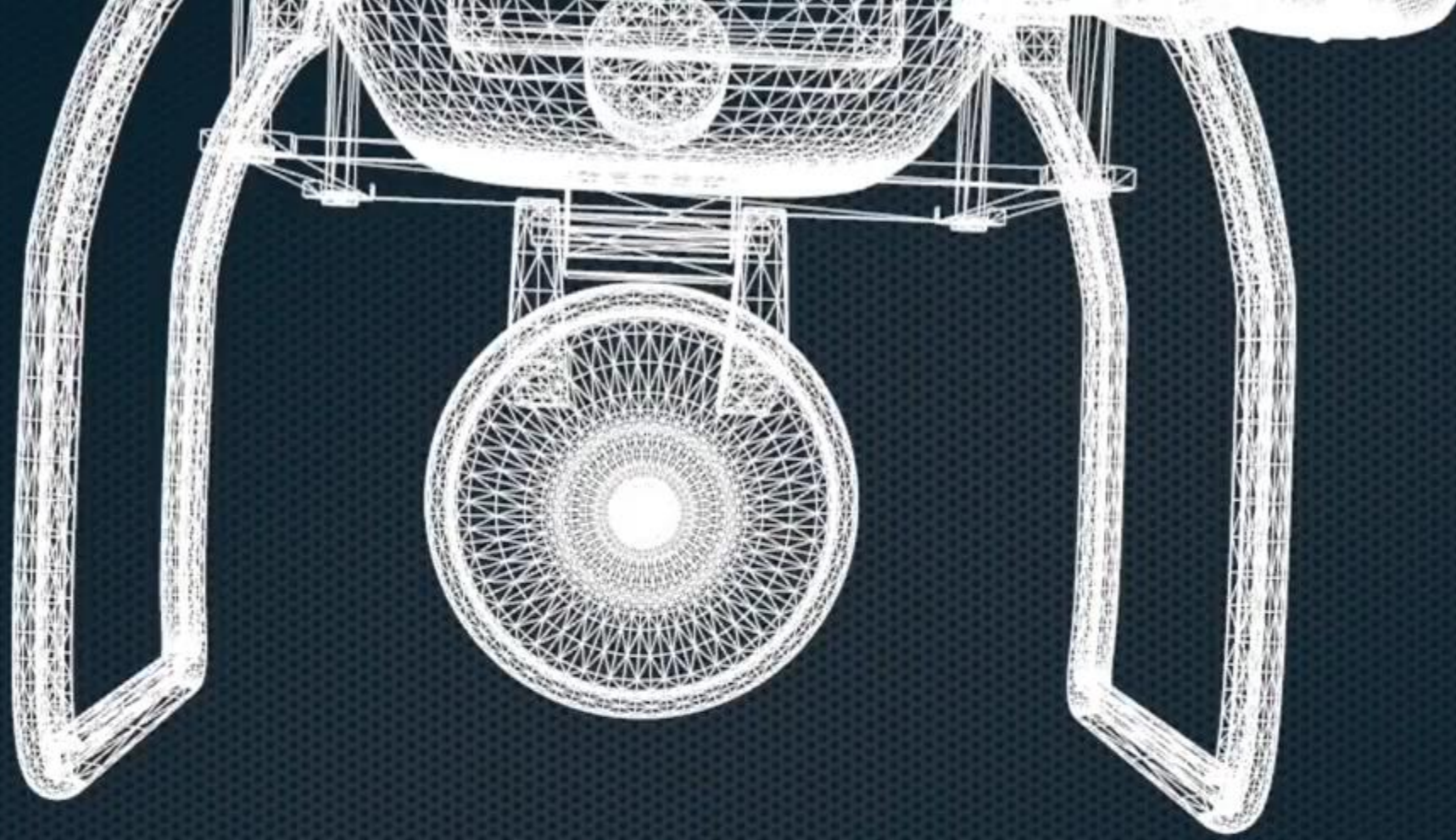


MOBILE SERVICES



CORPORATE RISK MANAGEMENT

Managing Risks Experience Day



Experience day
Drone detection / counter measures

Drones in Private Security



Opportunities

- Support guards in their missions, making them safer, more efficient and more secure
- Track, trace and monitor drones, like as is done with land vehicles, and respond to alarms given by drones
- Detect and prevent (also act) on ill-use of drones, unintentional or malicious

Securitas today:

- Drones used to support fire fighting at a large chemical plant. First response is to send the drone to obtain a verification of the situation and assess the potential risk to fire fighters and environment. Very fast intervention time. During fire fighting, the drone is used to fly behind the water wall and see where to concentrate the activities.
- Tethered drones used at large events to monitor the crowd and assess potential risks.



Threats

- As outlined in most recent CoESS doc, there is evidence of terrorist groups having used drones in the Middle East to drop bombs, transport illegal substance and spray hazardous chemicals (Tarin and Mustard Gas) => it's not a matter of **IF** but **WHEN, WHERE** and **HOW** drones will be used for terrorist or other criminal purposes.
- Cyber and IoT => hardware and software must be made very robust to resist hacking or in the future terrorist will easily create mayhem from behind a desktop. Hacking and directing one or more drones into Critical Infrastructure or planes comes to mind, but many more scenarios can be imagined by sick and determined minds.

CURRENT REGULATIONS FOCUS ON SAFETY, NOT ON SECURITY



Integrity | Vigilance | Helpfulness

www.securitas.com

