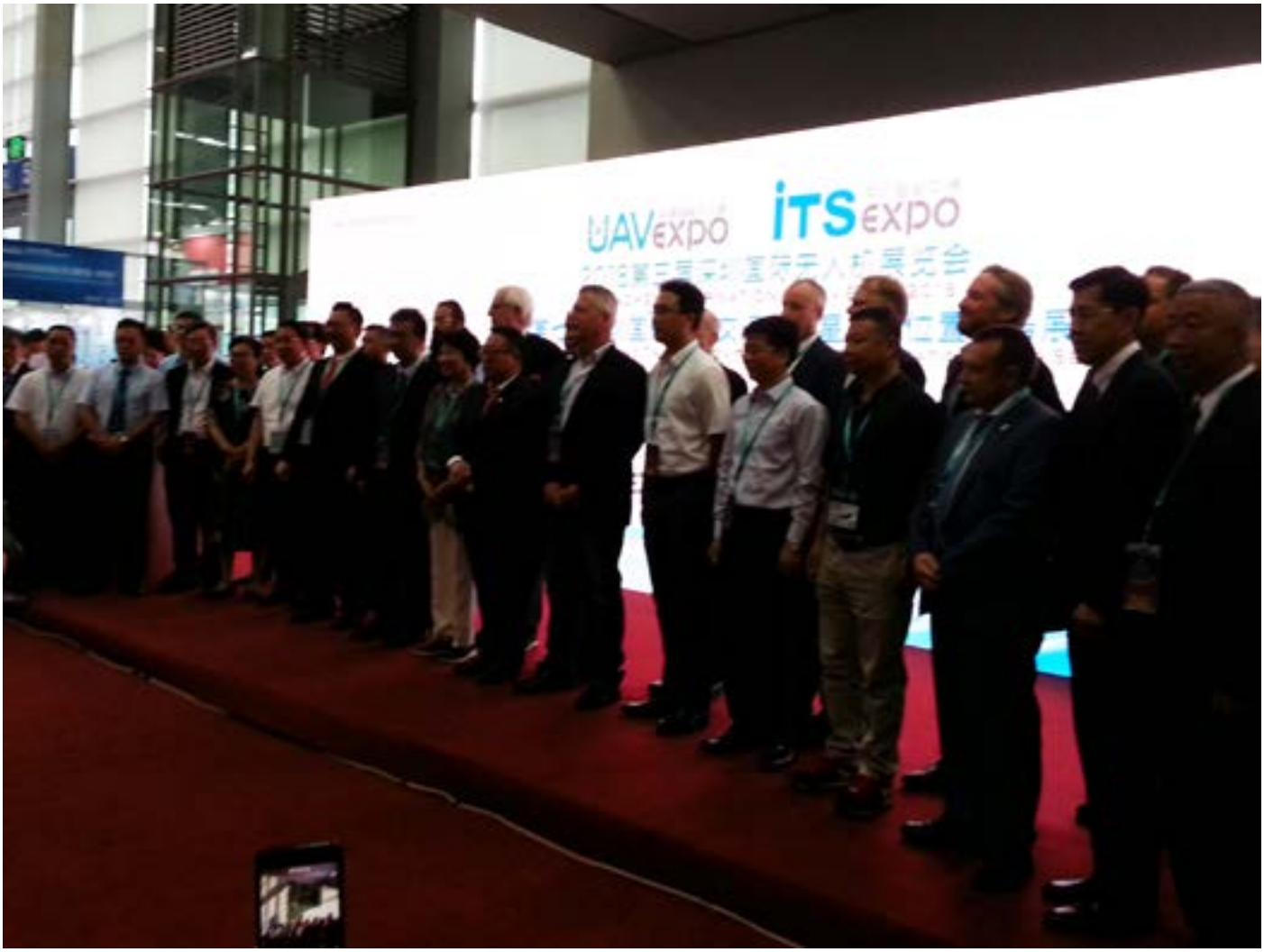
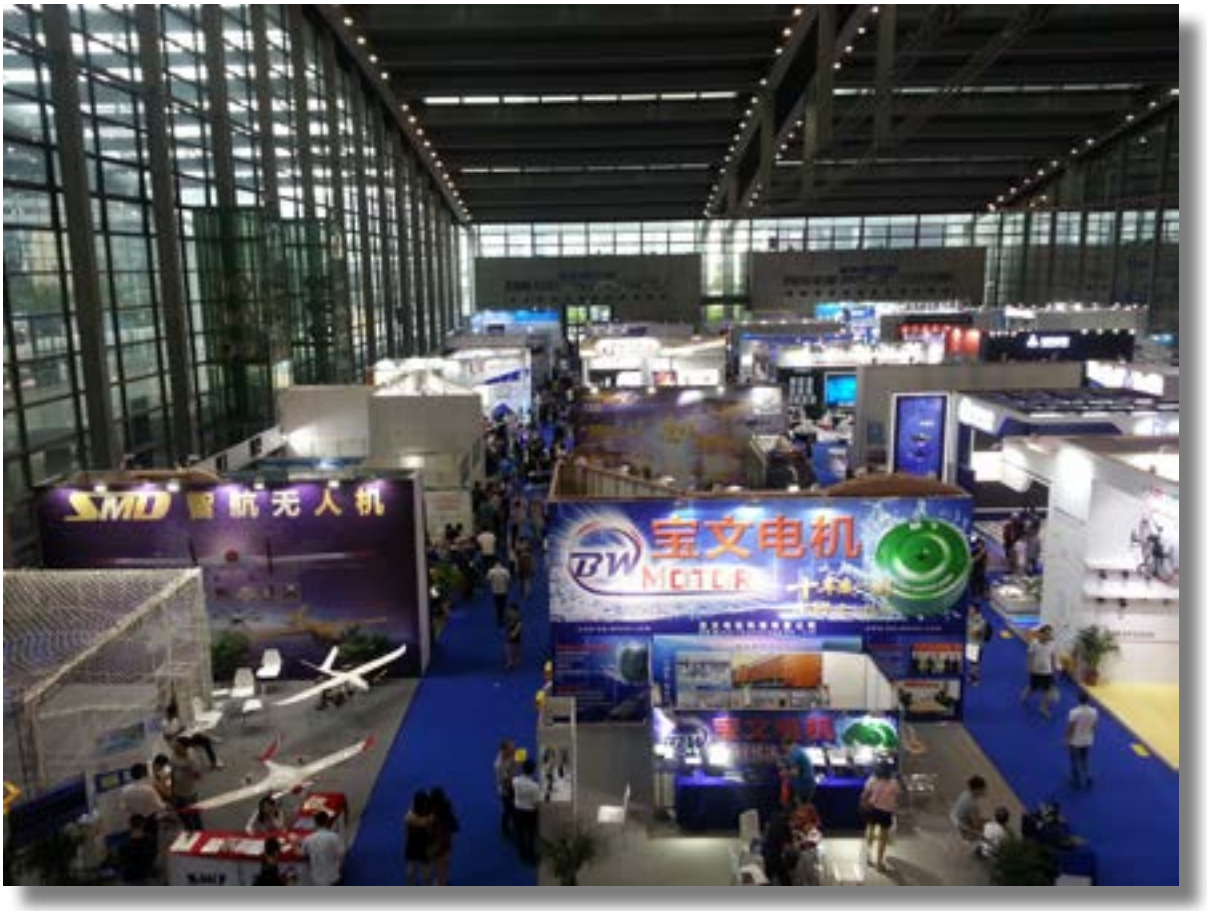
Drone Valley - Belgium



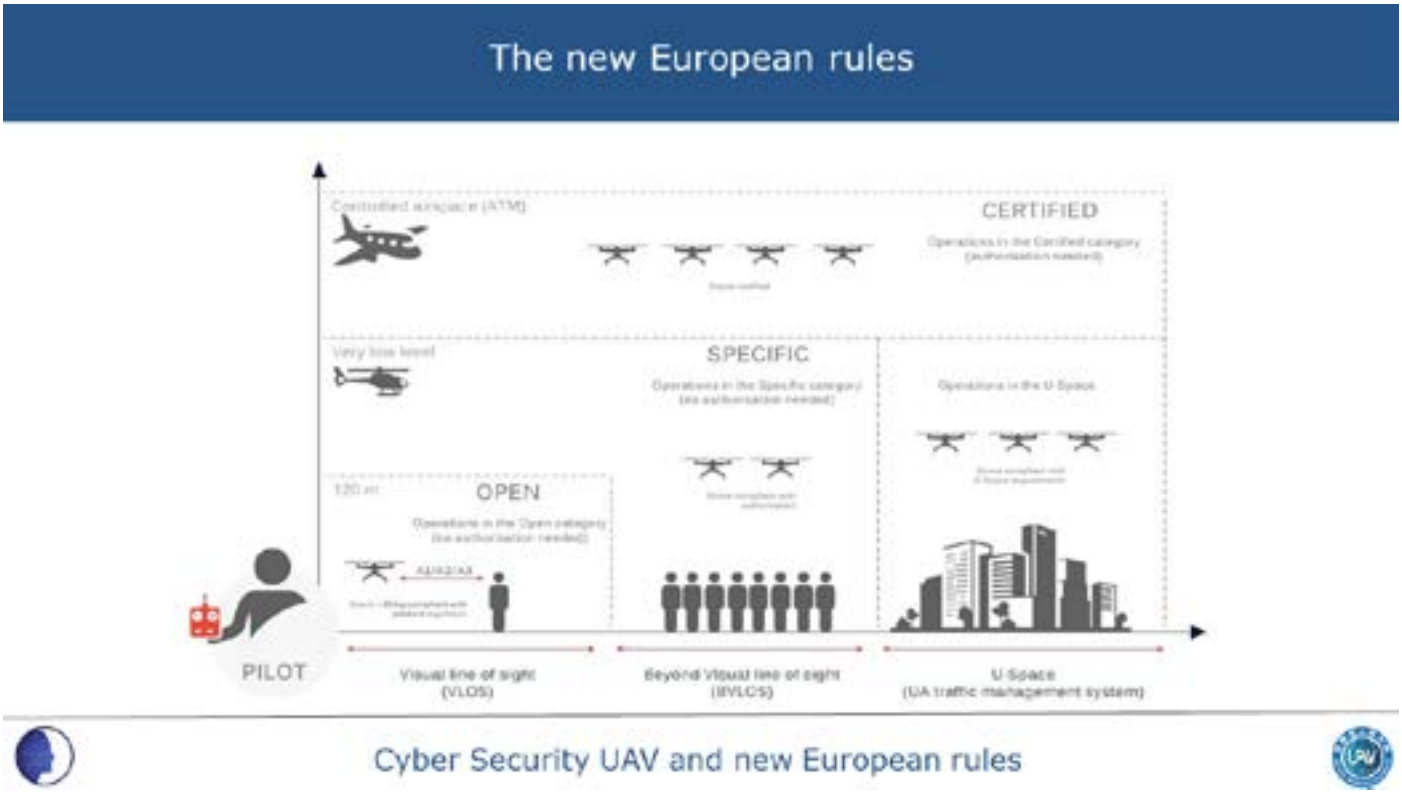
Shenzhen

The drone business in Europe…
A simple view of the future with an accident problematic if a strategy based on security and risk assessment is not implementedIt should be considered that a UAS operator may not be familiar with the aviation regulations and procedures.
(in particular, the information on the zones of a Member State should be made all available in a single source).

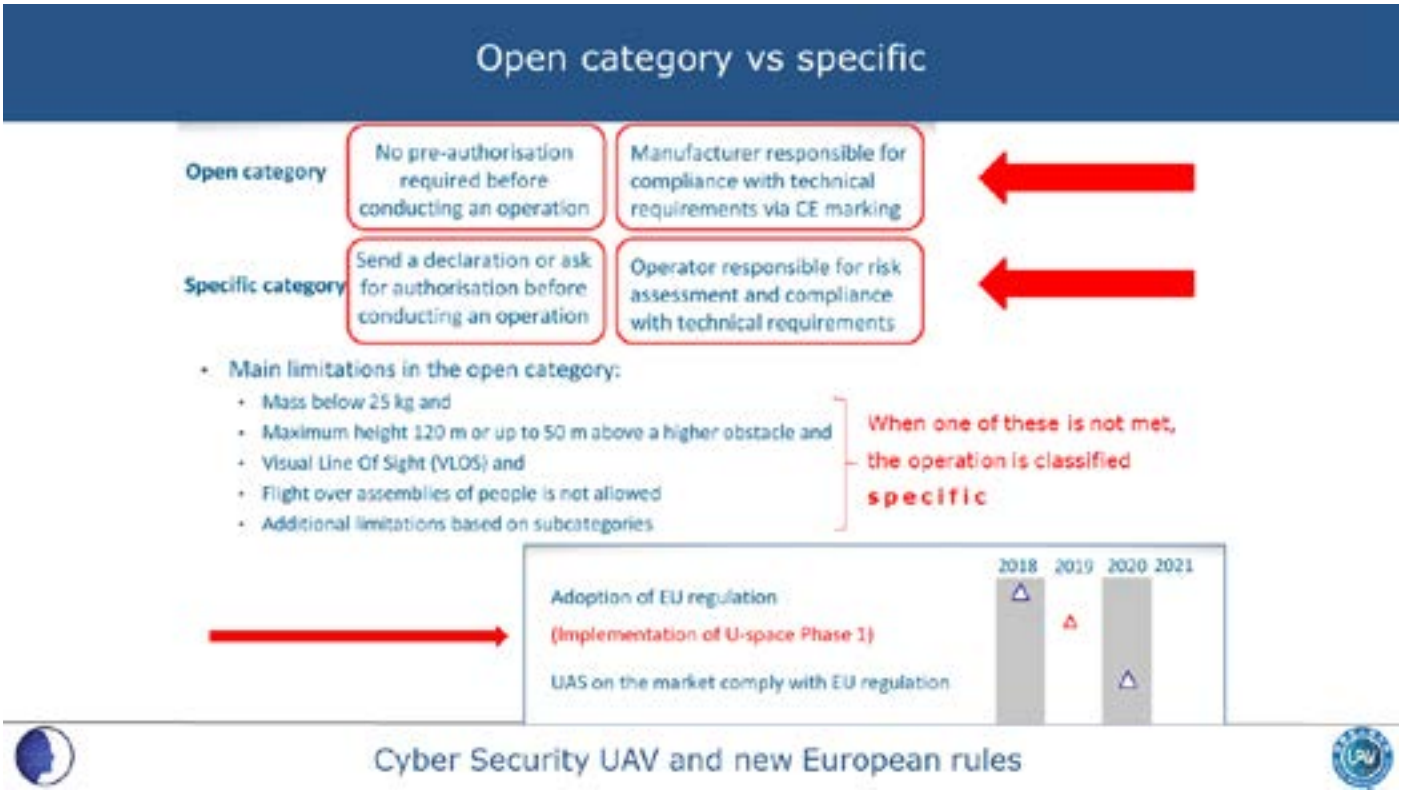


Why new European rules, apply to all EU countries
The uav sector is a great promesses for make many business and create jobs.One condition THE SAFETY FIRST !

Link for the video from (DroneRules.eu) : https://youtu.be/_s8AlyEI2p4

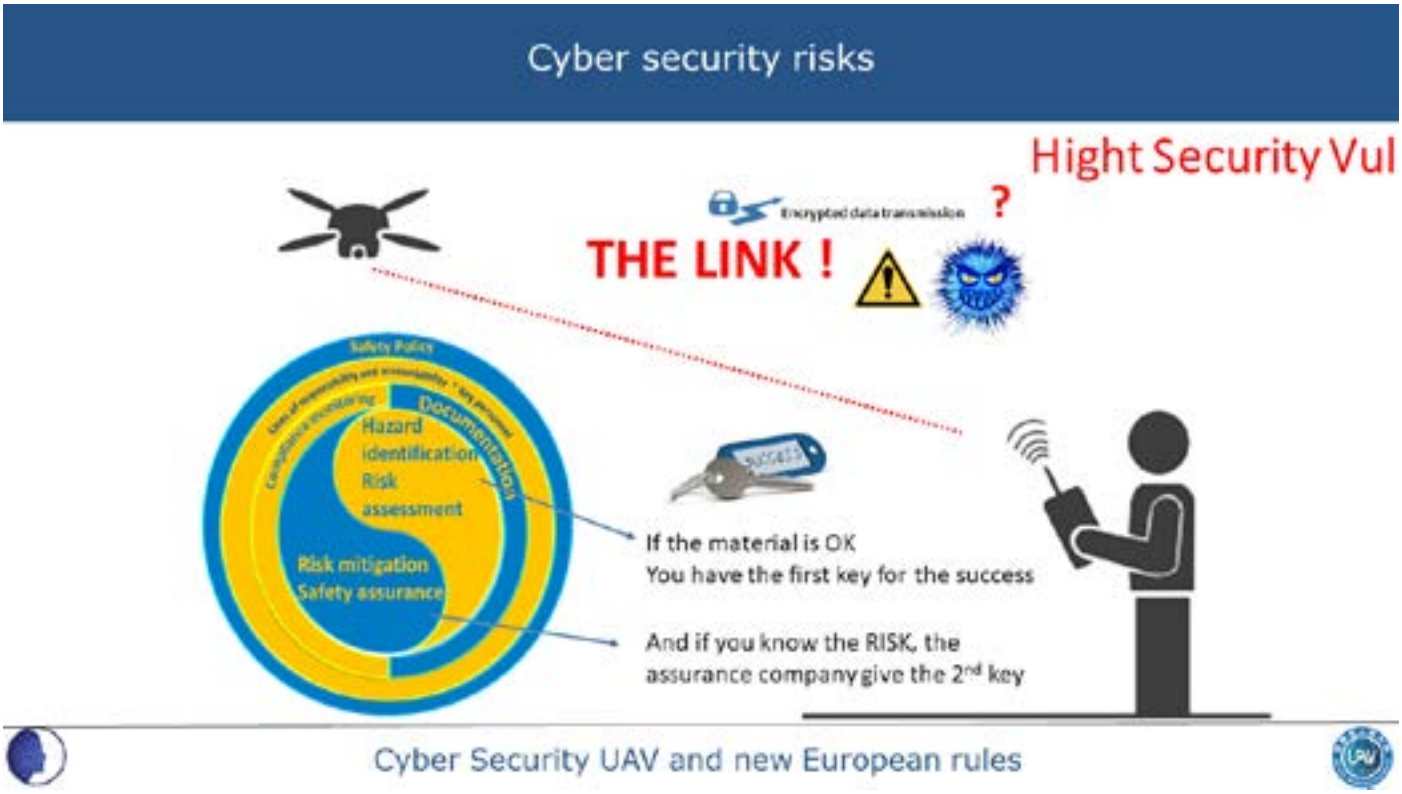


Quickly the european vision is simple.
3 class …
Open, Specific and Certified. Based of the RISKs.
Open caracterised by VLOS and 120m for the maximum altitude not flight over the people
Specific BVLOS a low level , flight over the people outside the city and for the next year the integration in the future U-Space IF the drone is certified (upgrade of the CE Homologation -> ISO)
And finaly the certified class … the ultimate level (not really definited today)



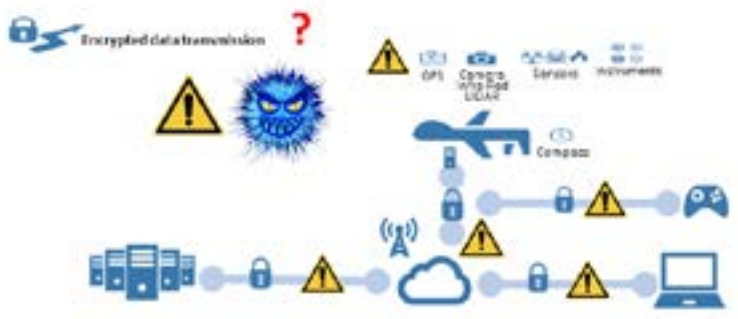
What's important today ?For OPEN categoryThe risk is reported on the manufacturer ...
CE marking and different technical requirements that correspond to ISO standards will be necessary to access the European market

For SPECIFIC categoryThe operator is responsible BUT he has to work with certified material!
You see the main limitation for the open category….
Your are quickly inside the SPECIFIC



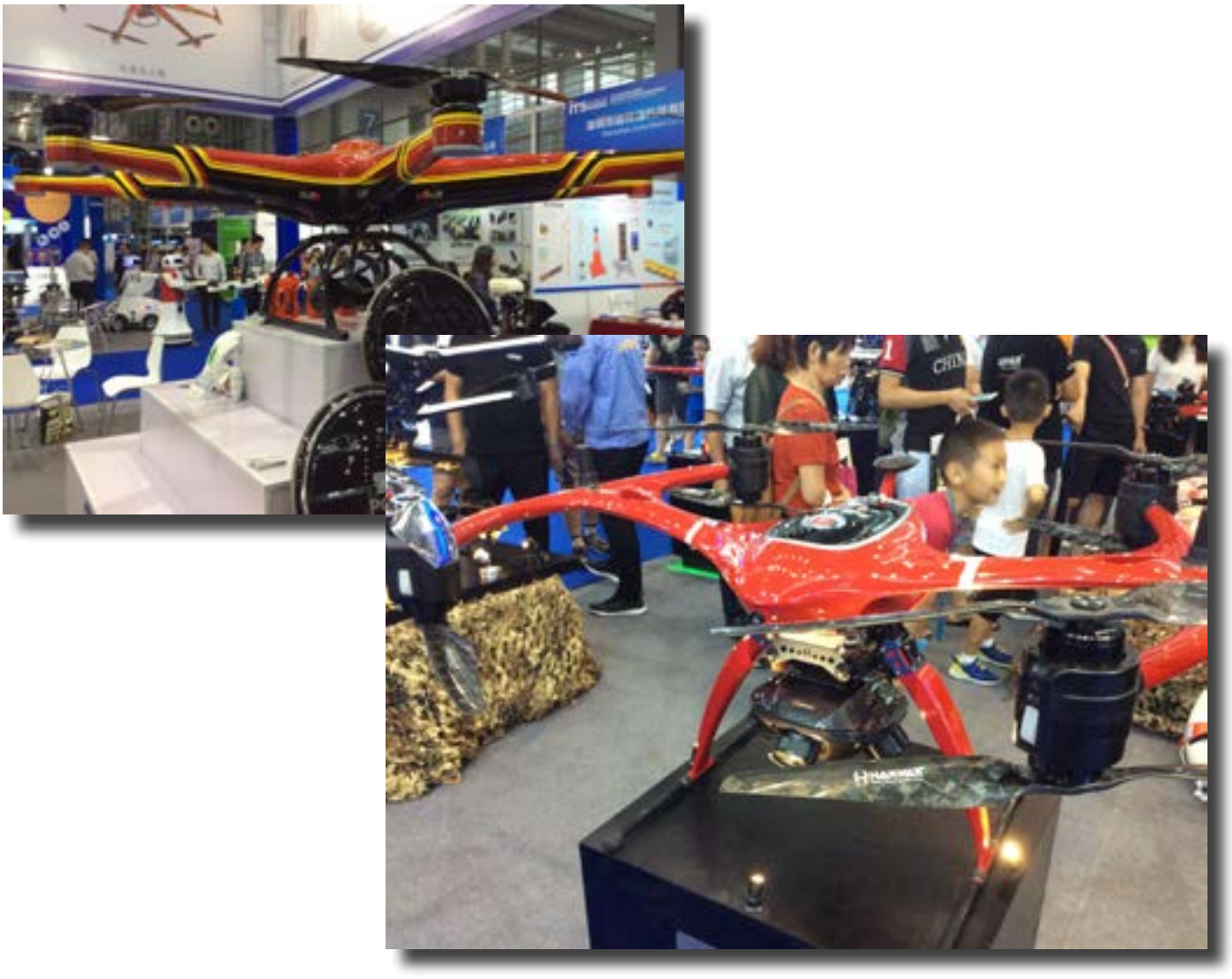
In the new rules … the cyber risk is very important
3 element to protect:
The command (simple radio control, phone/tablet or software inside a computer)
The UAV of course
And … the link !
The radio link is one of the entry points for malicious acts.
Although the data is encrypted, different techniques allow to pass this barrier.
(Sniffing and “Man in The Middle, …)
2 keys will be needed for insurance companies to analyze scenarios and associated risks.
In addition to the CE marking, the equipment must be analyzed to comply with the ISO standards for cybersecurity.
Operators should also be able to produce a risk analysis and propose solutions.
It will be necessary periodically to pass new tests according to the evolution of cyber risks

Potential Security Vulnerabilities



Cloud and proxy servers	Communications	Remote operations
Secured access Orchestration Archiving Advanced analysis	Satellite 3G / 4G / LTE Radio ...	Mission planning and follow-up Archive consultation Live telemetry feed Live image feed

We have identified various points sensitive to cyber attacks.
Not to mention the possible backdoors carried on board by the different loads…



Today many society in the cybersecurity sector working together and proposal a real great opportunity for manufacturer looking for a acces to the European market.

In the heart of Europe, in Belgium, in the south of the country, there are unique infrastructures and international skills.
We offer a testing and risk assessment center for manufacturers of drones, radio controls, various sensors.
UAS test sites and centres are becoming increasingly available for industry across Europe but until today, there are not yet premises devoted to Cyber Security assessment as CyTEF initiative.
The current test sites support companies and organisations in test campaign addressed mainly of navigation (GNSS) performance and certification with the purpose to use UAS in non-segregated airspace.

The interests for the UAS manufacturers, integrators and service providers are many, specially addressed to fill the gaps of their current test environments.
From one side, all the opportunities given by the CyTEF proposed facilities, could be carried on experiments using real assets. On the other side, the opportunity to make vulnerability assessment in cyber security domain for the UAS.

The Cyber Security is presenting challenges not even imaginable until now, because of the rapidly increasing of the drones' technology.Following CyTEF team analysis, currently there is a gap from industry needs and available test environments.
They are in most of cases internal labs of manufacturers while for integrators and providers there are only internal test for payload sensor's operation condition.

Needs of assessment of communication security from cyber-attacks is rising also by a recent study of McAfee:
2017 Threats Predictions, drones places threats in the sky (Dronejacking).
It reports, “Drones are well on the way to becoming a major tool for shippers, law enforcement agencies, photographers, farmers, the news media, and more.
Various researchers have found many consumer drones shipping with open ports and weak authentication methods, allowing a person with the right equipment to send commands to the victim’s drone.
The majority of the vulnerabilities discovered on commercial drones can be easily fixed with a software update; other is the IoT technology and devices including drones that have little or no security”.

More in general, the involvement of UAVs in commercial traffic and operating in both RLOS and BRLOS including satellite link, need secure communications and control of unmanned aircraft.
Cyber Security assessment is required also by recent publication of European Parliament, “Privacy and data protection implication in the civil use of drones”.
The document requested by the committee on civil liberties, justice and home affairs. It reports the risk for privacy and data protection by the UAS on-board video-cameras.

Further the increasing number of flying objects over airports, critical infrastructures and under authorization over cities pose a series of challenges and concrete risks for safety, security and the fundamental rights of persons, which are to be addressed seriously.

View CyTEF (Sat.infrastructures) in Redu (South of Belgium)

Our CyTEF Center will be propose a Cyber Security Test Range for the Aircraft System Assessment deploying ICT, EO, GNSS and Satcom System Infrastructure.

Cyber security should not be considered a but rather a process.
In order to support this process, it is important to be capable of describing and judging the security status of systems and making a risk assessment.
Then, put in place a mitigation procedure to reduce the severity of system impact.

CyTEF is addressed to the evaluation of cyber-attacks vulnerability and risks of UAS as a whole. It means flight platform; payload sensors; quality, consistency and authenticity of the data detected during the monitoring or surveying critical missions in extended scenarios BRLOS as well.
The CyTEF will be a complex infrastructure through which several types of UAS vulnerability and risk assessment services can be provided to the wide community of UAS manufacturers, operators and end users. In particular cyber vulnerability assessment services can be accessed by product manufacturers for analysis of innovative products any in the development phase or by UAS operators or end users to assess mission risks or data certainty.

CyTEF will be composed of a simulation environment and a real flight mission execution environment and airspace.
The cyber vulnerability of new products can be assessed by integrating mathematical models of innovative UAS or avionic/payload communication components in the simulation environment and simulating missions and results under cyber-attacks.
Furthermore, by leveraging test flight airspace and the Redu (south of Belgium) ground station, vulnerability of UAS and payloads can be assessed in real mission scenarios. The assessment services provided through the simulated environment is directly targeted to European product manufacturers (UAS, satellite and radio communication devices, avionic components) that can leverage the CyTEF services to model and test cyber performance of innovative products early in the product development cycle.
The services for vulnerability assessment in real mission scenarios are targeted to UAS operators and end users (but also to manufacturers ready to market UAS) that can access the services to verify security and safety of mission and of gathered data.
UAS vulnerability assessment is essential for evaluation flying mission risks and for certainty of gathered data.

Quality of data, in the end, impacts on the capability to correctly act during or at the conclusion of the missions.

We remain at your disposal for further information…

Cyber Security UAV and new European rules

Just a simple example of service offered by CYTEF
This company is an aviation auditor who offers various solutions related to ISO standards
After the analysis of the components by the test team, the information is transmitted to Q-Square for the drafting of the approval proposals…
An essential stage for access to the European market

Why ?
- Identify and mitigate risks
- Deliver on time on quality
- Reduce direct and non quality costs
- Optimize operations in the organization

Product Quality
- Airworthiness certificates (CSS, ARP 4754)
- Safety & Security (ARP 4761, IEC 61508, CE marking)
- Production & Maintenance (PART-21, PART-145)
- Electronic embedded systems (DO-254, ARINC)

What can we bring you ?

- Bring acute expertise in the interpretation of multiple & complex ASD standards
- Bring fresh and pragmatic ideas to settle smart and flexible processes
- 360° guidance setting up your Quality Management System
- 360° guidance driving your products to certification
- 360° guidance setting up your production and maintenance approvals
- Assistance in filling gaps with new referentials (e.g. EN 91XX:2016)
- Audit your suppliers and sub-contractors worldwide
- Develop and integrate your logistics support plans (ILS)
- Pilot your Quality Management System (ad-interim)
- Train your team and ease adoption

Next year we will have the 1st Platform for China in Wallonia (south of Belgium).
The CBTC … China Belgium Technology Center.
This is another opportunity to work together, as the CBTC will be the bridge between Chinese companies and EuropeWe will work closely with the CBTC teams to provide quick access to CyTEF services for UAS builders, radio control, etc.
A CBTC team is present in China and will liaise with the team in Belgium.
The latter will ensure communication between the parties concerned

Link for the video from : https://vimeo.com/248110530

Wallonia thinks partnership first !
China with its new economic projects is a key partner.
The new Silk Road, the Made in China 2025, demonstrates this willingness to collaborate and bring people together through technology

The best opportunity ...CBTC in Louvain-la-Neuve !
Alibaba moving to Liège Airport !
Air Belgium Charleroi, a new airline ...
First link via Honk Kong ... and forthcoming ... Shenzhen, Guangzhou, Beinjin ...
You are directly in the heart of Europe, after only 11 hours of flight

But Wallonia is not just business !
We also have beautiful historical sites…
Cities like Dinant, Namur, Bouillon ... the pearls of the wallonia !
We know that you also like to party .. by tasting traditional beers like the Trappists ...

You are welcome .... what are you waiting for ?

See you soon !

谢谢

Wallonie

Awex

@DroneValleyBEL

@Awex_Asia

#WALtechAsia

www.drone-valley.com

info@drone-valley.com

WeChat **DV2464**

digital wallonia .be

Avec le soutien de la Wallonie