EASA
European Aviation Safety Agency

Introducing the ESCP Strategy

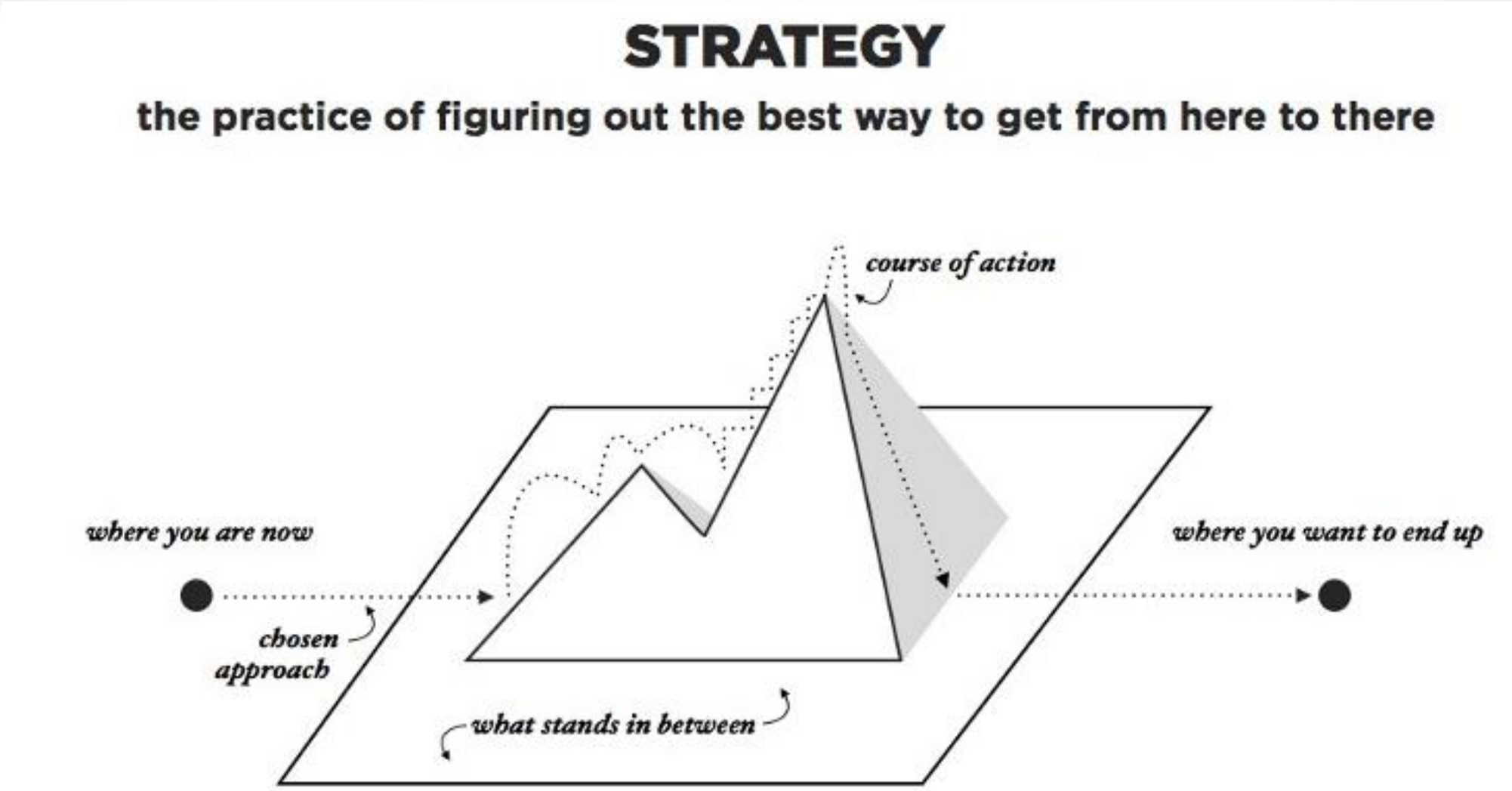
Davide Martini
Senior Expert - Cybersecurity in Aviation
Toulouse – 14th November 2018

Your safety is our mission.

An agency of the European Union

Our Approach

Strategy, in a few words…



Kernel Elements of ESCP Strategy

Diagnosis

An explanation of the nature of the challenge.
Know where you are and the final destination.

Guiding policy

An overall approach chosen to cope with or overcome the obstacles identified in the diagnosis.

Coherent actions

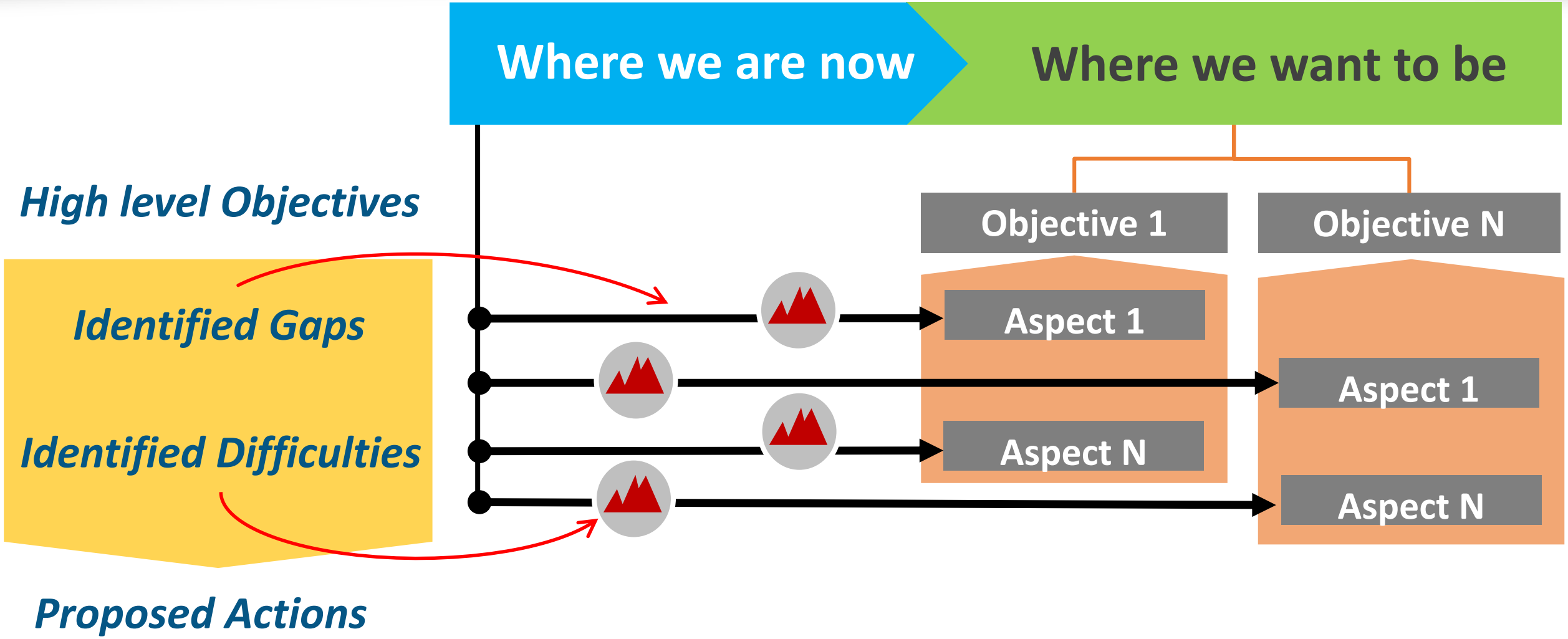
Steps that are coordinated with one another to support the accomplishment of the guiding policy.

Context and Working Plan

Working Method and Expected Outcome

ESCP Technical Advisory Committee (TAC) engaged

How the approach has been implemented



ESCP TAC Activity Overview

ESCP Vision – the starting point

To make the European Aviation System more resilient and more secure to cyber threats, by adopting a through-life tiered approach to security in design, production, operations and ultimately disposal of products, systems and services.

How can we translate this Vision in a more clear end point of our “journey”?

The Goal formulation

Where we want to be

The future aviation system will be a **trustworthy and dependable environment**, so that aviation stakeholders will be able to **rely on services and information provided by others** for the accomplishment of their operational objectives.

Guiding Policy

We will focus resources and actions to introduce a **systemic approach to cybersecurity** in aviation of **current and legacy systems** to develop a **system-of-systems capable to adapt** and therefore, to **withstand new threats without significant disruptions**.

The Goal formulation

Where we want to be

The future aviation system will be a **trustworthy and dependable environment**, so that aviation stakeholders will be able to **rely on services and information provided by others** for the accomplishment of their operational objectives.

Guiding Policy

We will focus resources and actions to introduce a **systemic approach to cybersecurity** in aviation of **current and legacy systems** to develop a **system-of-systems capable to adapt** and therefore, to **withstand new threats without significant disruptions**.

Main Strategic Directions

Guiding Policy

We will focus resources and actions to introduce a **systemic approach to cybersecurity** in aviation of **current and legacy systems** to develop a **system-of-systems capable to adapt** and therefore, to **withstand new threats without significant disruptions**.

1st Direction

Making Aviation an evolutionary cyber-resilient system

2nd Direction

Making Aviation self-strengthening by adopting a "built-in security" approach

Strategy Timeline

When do we want to reach the Goal?

Ideally… Tomorrow

More realistically, ESCP members want to have
an idea of the required effort –> ***Effort Driven Plan***

Formulation of Strategic Objectives 1/2

Making Aviation an evolutionary cyber-resilient system

- **Operations continuity assurance is enforced with distributed protection along functional chains**
- **Operational Systems can fail gracefully by ensuring continuity of essential services**
- **Operational Systems adopt multi-layered protection measures that hinder the progress of an attack**
- **Aviation stakeholders understand the trans-organisational nature of Aviation system and make use of connections to collaborate**

Formulation of Strategic Objectives 2/2

Making Aviation self-strengthening by adopting a "built-in security" approach

- **Systems design practices are in place to avoid unintended use of functions exposed to users**
- **The consequences of unauthorised interactions are assessed and managed by design, also enforcing adaptive protection measures**
- **Assurance and scrutiny processes allow for the security effectiveness of systems during the whole lifecycle**
- **The level of protection against external causes is assessed periodically and, if necessary, restored**

The Strategic Actions Plan

The strategy will include, among others, actions in the following areas:

Coordination

Technical

Regulation

Standard/Methodology

Capacity Building

Steps to Strategy Endorsement

Three Steps Proposed

1. Finalise the **Actions Plan** – Today's discussion is a key
2. Finalise the **Effort** and the **Operational Roadmap**
3. **Endorse the Strategy** and **implement the Roadmap**

EASA
European Aviation Safety Agency

Thank You!

Your safety is our mission.

An agency of the European Union

Practical elements of Resilience

KEY ELEMENTS

Identify critical services and scenarios that could impact

Build layered systems and allow partial and recoverable failures

Stay networked to predict new threats and be prepared

Protect Crown Jewels

Avoid Domino effect

Collaborative Intelligence

Resilient system to handle attacks: key points until 2025

MILESTONES (approx. timeline) — 2018

Aviation is an evolutionary cyber-resilient system

Aviation adopted "built-in security" and works on self-strengthening

Coordination

- Discuss shared trans-organizational risk management (STORM)
- Discuss trans-organizational resilience targets and service levels
- Agree on common risk acceptability criteria in support of the dependability and trustworthiness of systems and services
- Discuss stakeholders needs, legal basis and policies for collaboration and info sharing
- Agree upon responsible disclosure process in reaction to vulnerability discovery from researchers, or third parties.

Technical

- Develop a European Centre for Cybersecurity in Aviation
- Discuss needs for design practices improvements and related research activities

Standards & Method.s

- Implement an Information Security Management System (ISMS)
- Introducing cyber-disaster response and recovery capabilities for operations
- Evaluate need for regulating cybersecurity objectives of interconnected systems and services
- Finalise Industry Std.s under development and advice for new needed guidance
- Finalise Industry Std.s EN16495

Regulation

- Develop a European Regulation framework for Information Security in Aviation
- Evaluate need for regulating cyber-disaster response capabilities
- Introduce in the Certification Spec.s and/or AMCs cybersecurity provisions
- Evaluate need for regulating the process for remediation of cybersecurity vulnerabilities including related certification issues.

Capacity Building

- Deliver tailored training courses to executives
- Produce Learning Objectives for Cybersecurity in Aviation
- Deliver awareness sessions and tailored training courses to professionals
- Encourage introduction of cybersecurity in aviation courses in academic syllabus
- Discuss ongoing cybersecurity research activities and consider outcomes for improvements
- Support or develop research activities aimed at exploring safety and security interactions.