ASECAP DAYS

PARIS 2017

## 45TH ASECAP STUDY & INFORMATION DAYS 2017

# The Concession model in the decarbonization era: preparing the infrastructure of the future

*Pullman Paris Montparnasse Hotel*
*29-31 May 2017*

**www.asecapdays.com**

Organized by

ASECAP

ASECAP DAYS

PARIS 2017

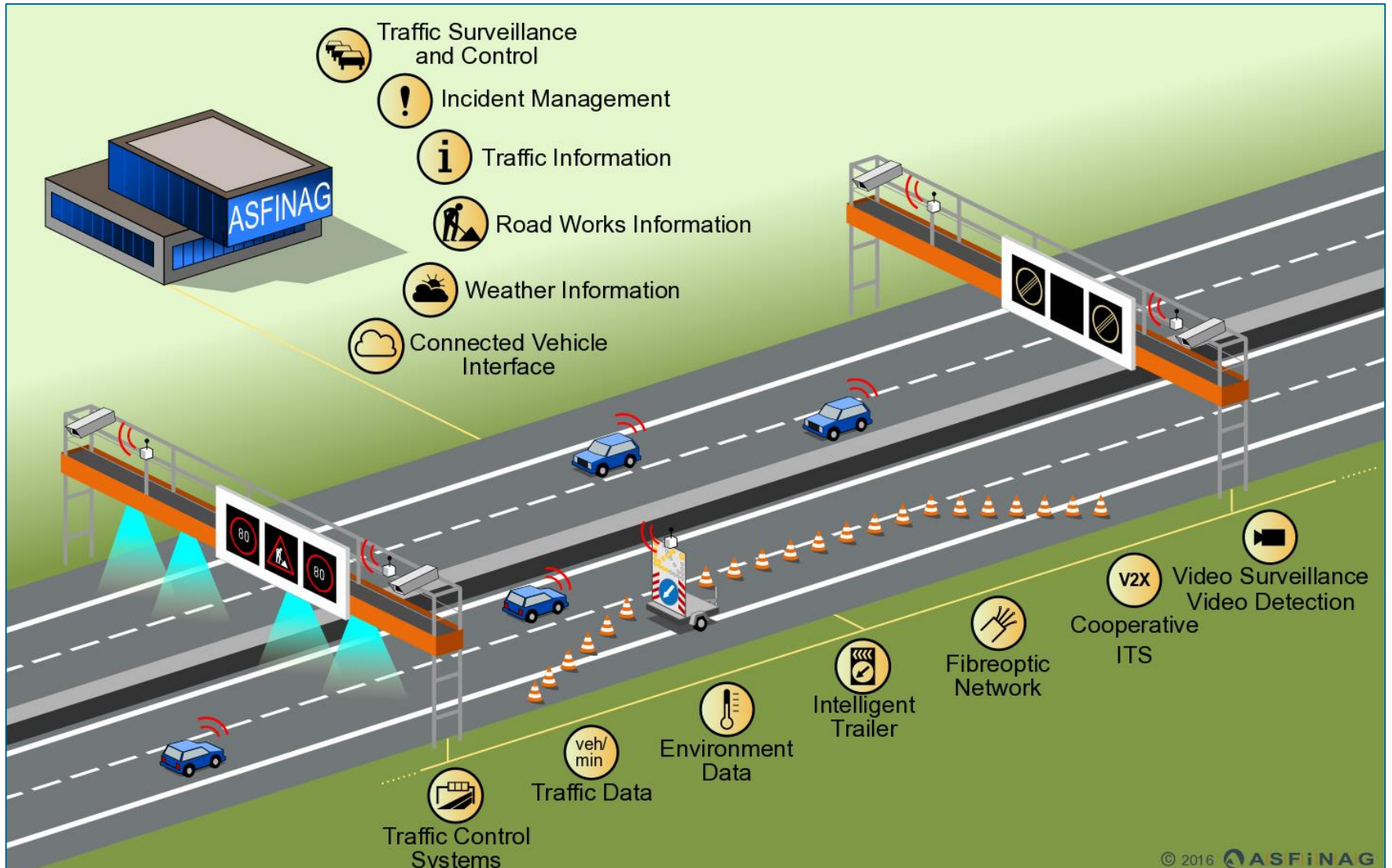
*45TH ASECAP STUDY & INFORMATION DAYS 2017*

# ASFINAG's approach and activities to raise the security level of network and information systems

*Directive to ensure a high level of common network and information security in the Union*

**www.asecapdays.com**

# Digital infrastructure is the basis for innovative services but offers many possible targets for cyber attacks



# Cyber attacks become more sophisticated and change in type

- Business disruption attacks increase
  - Data leakage/theft
  - Destruction /manipulation of infrastructure management systems
  - Denial of service attacks towards web based systems
- Attacks on network devices
- Targeted attacks
- Ransomware
- …

=> Telematics infrastructure suppliers are usually not prepared for increased rate of dynamics in cyber attacks

# Network and Information Security Directive of the European Union (NIS-D) applies to ASFINAG

ASECAP DAYS
PARIS 2017

- Shall ensure a high level of common network and information security in the European Union
- Applies to “operators of essential services” that rely on IT e.g. traffic management and traffic information
- National implementation of guidelines by April, 9th 2018
- Specifies organizational measures
    a. national strategy for the security of network and information systems;
    b. a network of computer emergency teams (CSIRT-Computer Security Incident Response Team);
    c. the introduction of a reporting obligation for certain sectors
- Specification of security requirements for operators of “essential services” in specific sectors

# Consequences for operators of essential services

- Introduction of IT Risk management
  - appropriate, proportionate technical and organizational measures to deal with the risks
- Documented information of authorities, how the operator complies with the security requirements
- The proof can be provided by a certified information security management system (ISMS)
- The authority or a qualified auditor may investigate the effectiveness of the security measures
- The authority may issue instructions how to deal with the identified deficiencies
- Operators of essential services must report to the authorities security incidents that have a significant impact on the availability of the service

# Project SHIELD was set up to further increase IT-security at ASFINAG (1)

Introduction of

- a group-wide information security management system (ISMS)
- an IT risk management linked to overall risk management
- next generation firewall, intrusion detection and intrusion prevention
- Security Information & Event Management (SIEM) -> Detection & Alarming
- Privileged Identity & Access Management (PIAM) -> administrator access can be logged/managed
- network traffic pattern analysis

Segmentation of data network to reduce overall damage in case of IT-security incidents

# Project SHIELD was set up to further increase IT-security at ASFINAG (2)

- Detect and resolve existing IS vulnerabilities in all ASFINAG systems
  - Identification of existing weak points
  - Technical hardening of information security of existing installations
- Prevention of future information security vulnerabilities
  - Requirements definition and implementation of a network security concept
  - Requirements for procurement of IT-related components to ensure information security
- Implementation of central IT-services for traffic management and telematics infrastructure regardless of suppliers

# Central services and standard building blocks in each tunnel reduce IT-risks and improve manageability