

Creazione di un ISAC (*Information Sharing and Analysis Centre*) nazionale per il settore del trasporto stradale

Alessandro Musmeci

La rete autostradale in concessione: Associate AISCAT e altre Società autostradali

17 Associate

[su un totale di 26 Società Concessionarie]



4.613,1 km in esercizio
[Totali = 6.097,4 km]



1.727,0 km 3 o più corsie
[Totali = 1.960,1 km]



70,8 Mld Veic*km (Tp= 24%)
[Totale = 86,7 Mld Veic*km (Tp = 23%)]



1.113 Ponti e Viadotti⁽¹⁾ (Lunghezza tot= 519,1 km)
[Totale = 1.679 Ponti e viadotti⁽¹⁾ (Lunghezza tot = 897,3 km)]



531 Gallerie⁽¹⁾ (Lunghezza tot = 627,2 km)
[Totale = 717 Gallerie⁽¹⁾ (Lunghezza tot = 851,7 km)]



3 Trafori Internazionali (Lunghezza tot = 25,4 km)



(1) Gallerie, ponti e viadotti con lunghezza > 100 m

L'interconnessione tra Società Concessionarie



- **22 Società interconnesse (su 26, più di 5.000 km di rete)**
- Non c'è la percezione di trovarsi in un sistema gestito da diverse Società: **operatività come un unico network (peculiarità italiana)**
- **Superata la frammentazione "fisica" tra le varie concessioni (inizio anni '90)**
- **Elevata interoperabilità nel funzionamento e negli standard tra le diverse tratte, non solo limitata all'esazione ma estesa anche ai sistemi di sicurezza e gestione dei flussi**
- ❖ **Protocollo di Intesa** (aspetti procedurali, legali, gestionali, tecnici)

Esempio: viaggio Aosta-Taranto

- 1.246 km
- Almeno 4 società attraversate

Sistemi Intelligenti di Trasporto (ITS)

- ✓ Gli ITS esistono in funzione della strada e sono uno strumento fondamentale per il gestore autostradale per contribuire a migliorare le condizioni di mobilità e di sicurezza lungo la rete autostradale e ottimizzare la gestione della rete
- ✓ Le concessionarie italiane sono da sempre in prima linea nella ricerca e nell'implementazione di nuovi e più efficienti sistemi tecnologici

37 Centri di Controllo del Traffico (24/7)

1.482 Centraline meteo e rilevatori ghiaccio/nebbia

8.543 Colonnine SOS

13.051 Telecamere lungo la rete

Call Center Viabilità e Numeri dedicati

4.070 Pannelli a Messaggio Variabile



ISAC (*Information Sharing and Analysis Centre*)

ENISA definisce ISAC come un'organizzazione no-profit che:

- ⇒ faciliti lo **scambio di informazioni** su **minacce informatiche** relative a **specifiche infrastrutture critiche** (come quelle autostradali), su **incidenti e cause scatenanti**, nonché su **esperienze e buone pratiche** nel campo della cybersicurezza.
- ⇒ fornisca adeguato **supporto alle Istituzioni competenti** per la **definizione di norme e regolamenti**, attraverso la **condivisione di requisiti di sicurezza informatica e contromisure comuni**
- ⇒ rappresenti anche il “luogo” dove **centralizzare servizi quali accordi e protocolli tecnico-operativi** e nel quale stabilire le **specifiche di mercato**

Definition and sharing of
guidelines

Definition of technics and
technologies to implement
the guidelines and drive
investments in cybersecurity

Report and Monitor each
component's residual risk

ISAC (*Information Sharing and Analysis Centre*)

Nell'ambito della Strategia Nazionale di Cybersicurezza 2022-2026, predisposta dall'Agenzia per la Cybersicurezza Nazionale (ACN), assume particolare rilevanza la promozione di **iniziative di carattere pubblico-privato finalizzate a favorire il potenziamento dello scambio informativo e di best practices tra Pubblica Amministrazione e operatori economici privati**

STRATEGIA NAZIONALE DI CYBERSICUREZZA



Misura #34: Creazione di un **ISAC nazionale** per abilitare lo scambio di informazioni e analisi di minacce cyber con gli stakeholders



Misura #35: Promuovere la creazione di **ISAC settoriali** integrati con ACN ISAC



OBIETTIVI DI ISAC ITALIA



Incrementare la cyber resilienza attraverso la condivisione di informazioni strategiche di alto livello come best practices, analisi e linee guida



Promuovere la cultura della cybersecurity e migliorare la consapevolezza dei settori pubblico e private come società civile in ambito del rischio cyber e delle relative minacce



Facilitare la creazione di ISAC settoriali allo scopo di sfruttarne l'esperienza di settore nella gestione delle minacce cyber



ISAC (*Information Sharing and Analysis Centre*) di settore

In questo quadro, in ottemperanza della Misura #35 del Piano di Implementazione della Strategia, si inserisce il progetto di creare, in sede AISCAT, un ISAC del settore del trasporto stradale



Qual è il contesto

- La UE 2016/1148, prima, e la UE 2022/2555 (“NIS 2”), poi, classificano come **settori ad alta criticità** (allegato I, 2, 2 (d)):
 - **Le autorità stradali responsabili del controllo della gestione del traffico**
 - **Gli operatori dei sistemi di trasporto intelligenti** (cfr. art. 4, punto (1), della Direttiva 2010/40/UE)
- Revisione della Direttiva ITS e legame con la NIS
- Regolamenti relativi alle informazioni di traffico (cfr. Safety Related Traffic Information, SRTI, o Real Time Traffic Information, RTTI)
- Forme di scambio informativo tra Società concessionarie (es. collaborazione all’interno di progetti europei quali C-Roads e Napcore)
- Normative ed esperienze già avanzate per altri settori, come il ferroviario (CENELEC CLC/TS 50701), il marittimo, o il sanitario (IEC TR 60601-4-5, 81001-5-1)

Come definire cosa proteggere, qual è la tassonomia dei servizi essenziali, qual è la definizione di impatto rilevante, quali ricadute sul sistema?

ISAC (*Information Sharing and Analysis Centre*) di settore

Gli operatori autostradali condividono servizi digitali con elevata criticità:

- ⇒ **Sistemi IT/Ambienti cloud**, endpoint, server (solitamente con rete in fibra dedicata)
- ⇒ **Strutture fisiche IT**, sistemi di fornitura energetica, alimentatori, cavi energetici
- ⇒ **OT/IoT/Core Business**, connesso, tra gli altri, a funzionamento delle infrastrutture critiche, riscossione elettronica dei pedaggi, stazioni di ricarica, ITS, gestione del traffico e PMV
- ⇒ **Sistemi di automazione gallerie** e impianti relativi

- Finora, al di là di collaborazioni territoriali, gli operatori hanno implementato le eventuali contromisure in maniera indipendente, ponendo un problema di trust organizzativo e tecnico: **gli operatori autostradali sono connessi** e si scambiano informazioni relative alla programmazione del traffico, sistemi di trasporto intelligenti e **sicurezza**.
- La presenza di una norma scritta dagli esperti di settore è la base per il raggiungimento di obiettivi condivisi, sia sulla creazione di architetture di sicurezza robuste, sia sullo sharing delle informazioni relative ad eventi cyber e contromisure.

ISAC (*Information Sharing and Analysis Centre*) di settore

- ✓ **Evitare gli effetti a cascata:** la creazione di un ISAC, con i rispettivi *game days* di simulazione di incidente, renderebbe efficace la risposta ad un attacco che inizia da un operatore e si trasferisce ad altri, e supporterebbe le relative analisi attraverso *Multi-Sectorial Assessments*
- ✓ **Ottimizzare la conoscenza:** un ISAC regolato garantirebbe, *day by day*, lo scambio di informazioni, e aiuterebbe anche le realtà più piccole, meno strutturate
- ✓ **Adeguare e potenziare gli strumenti a disposizione:** generalmente le soluzioni di sicurezza fornite sono disaccoppiate fra loro, rendendo difficile lo scambio di informazioni in formato standard. È opportuno conoscere i vari strumenti per capirne il funzionamento in caso di incidente

