



The Value of Connections

Turning Cyber Security Threats into Strategic Resilience

Interferry Conference 2025
RINA

Our experience. Your growth.

Ship Assets and Criticalities



A ferry is a **Computer-Based “System of Systems”** pertinent to OT & IT domains

Class and SOLAS requirements only cover **part of the assets** (E22/E26/E27)

On board it is possible to find other critical systems (monitoring, communication, commercial support...) not covered by ISM/ISPS/Class having **direct impact on operational continuity** meaning the **ferry can or cannot sail and be operated as expected**

A complete **Asset Inventory Categorization Mapping** is essential

Risk Mapping Methodology



1. Scoping & Categorization

- OT
- IT
- Critical Assets
- Continuity Systems

2. Threat & Vulnerability Mapping

- cyber + non-cyber connectivity
- complexity
- human factors

3. Risk Evaluation

(Rec. 171) Likelihood × Impact



4. Business Impact Analysis

- ISO 22301/22317
- Determining the maximum tolerable period of disruption
 - Definition of RTO and RPO
 - Mapping of processes dependency

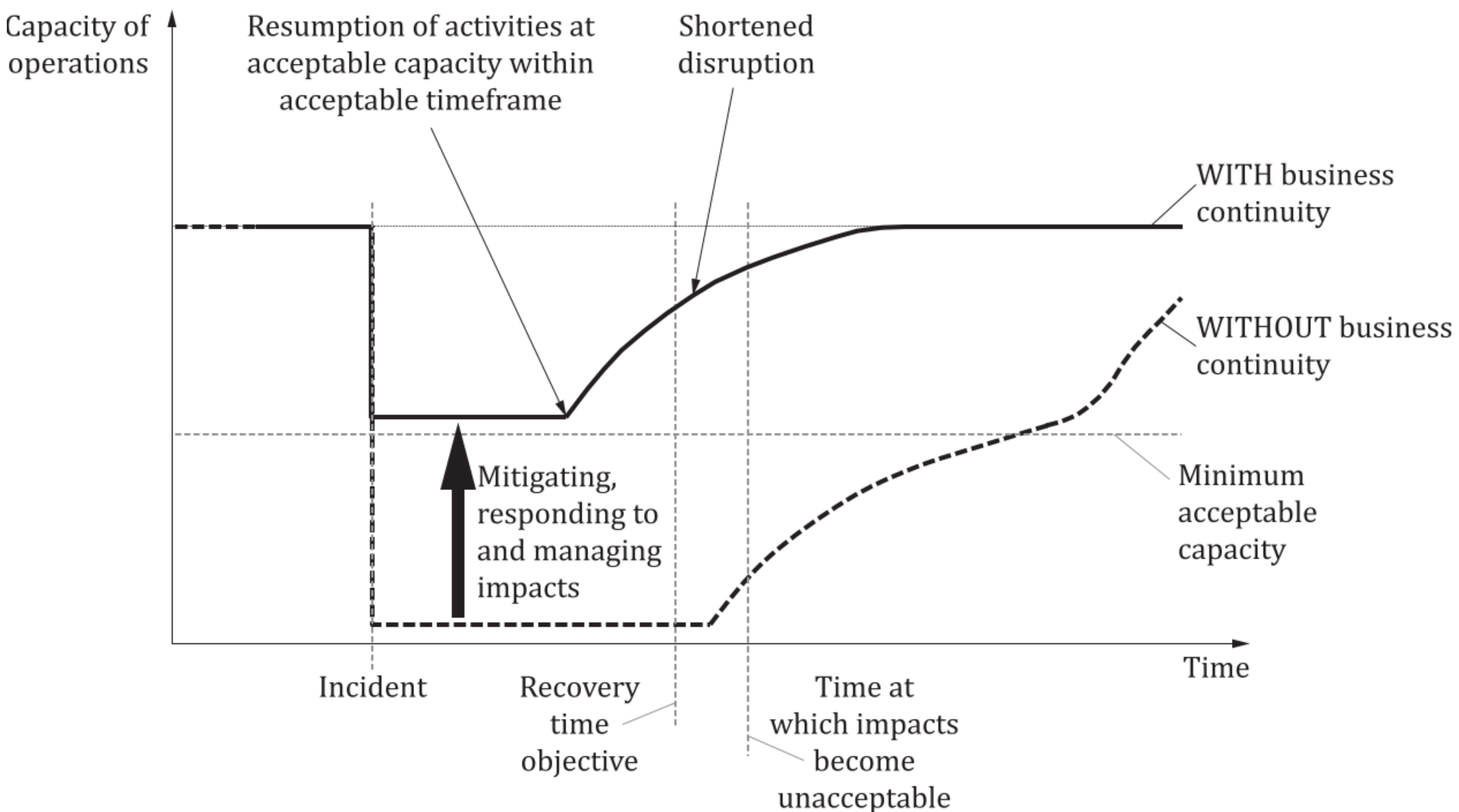
What would ships look like to hackers?

COMMS	Email, Radio, Ship-to-Shore Ship-to-Ship, Voip	Updates & Remote administration	ADM
NAV	Radar, Charts/ECDIS, Route planning, Weather system, GPS, Gyros	Email, Stores, crew timekeeping, Customs, EES, malware resistance, USB, PMS, payroll	SHIP NET
		Server rooms, Mach. Spaces, Network infra., social eng, Access control, Bridge, Hotel	PYS.
		Stability, deck planning, Hull stress monitoring, ballast system, EDIFACT mex	LOAD
		Firewalling, Segmentation devices	SECURI.
		HMIs, Airgap, PLCs	ICS

Business Impact Analysis Principles & Examples



Ex: Business continuity for sudden disruption



OT Systems :

- Propulsion
- Power Generation
- Navigation Equipment
- Safety
- Communication

IT Systems:

- Load & Stability & Stress Monitoring
- Booking
- Shops & Entertainment
- Security
- Planning Maintenance Systems
- Connectivity

The list of systems at risk is longer!

Benefits of the Integrated Approach

CYBERSECURITY IN FERRY SECTOR

Define the roles and responsibilities of users, key personnel and management both ashore and aboard.

01

Identify systems, assets, data and capabilities that, if breached, could pose a threat to the operations and safety of the ship.

02

Implement technical and procedural measures to protect against cyber incidents and ensure business continuity.

03

Carry out activities to prepare for and respond to cyber incidents.

04

An umbrella overview integrating:

- IACS Rec.171
 - URs E26 / E27
- and
- ISO 22301

into a true value enhancer for your assets

Asset Visibility

database with categorization and criticality ratings

Risk-to-Business Mapping

link cyber risk to operational and reputational impact

Strategic Prioritization

allocate mitigation resources to the most critical assets

Continuity & Resilience

response and recovery strategies validated through exercises (ISO 22301 - 8.5)

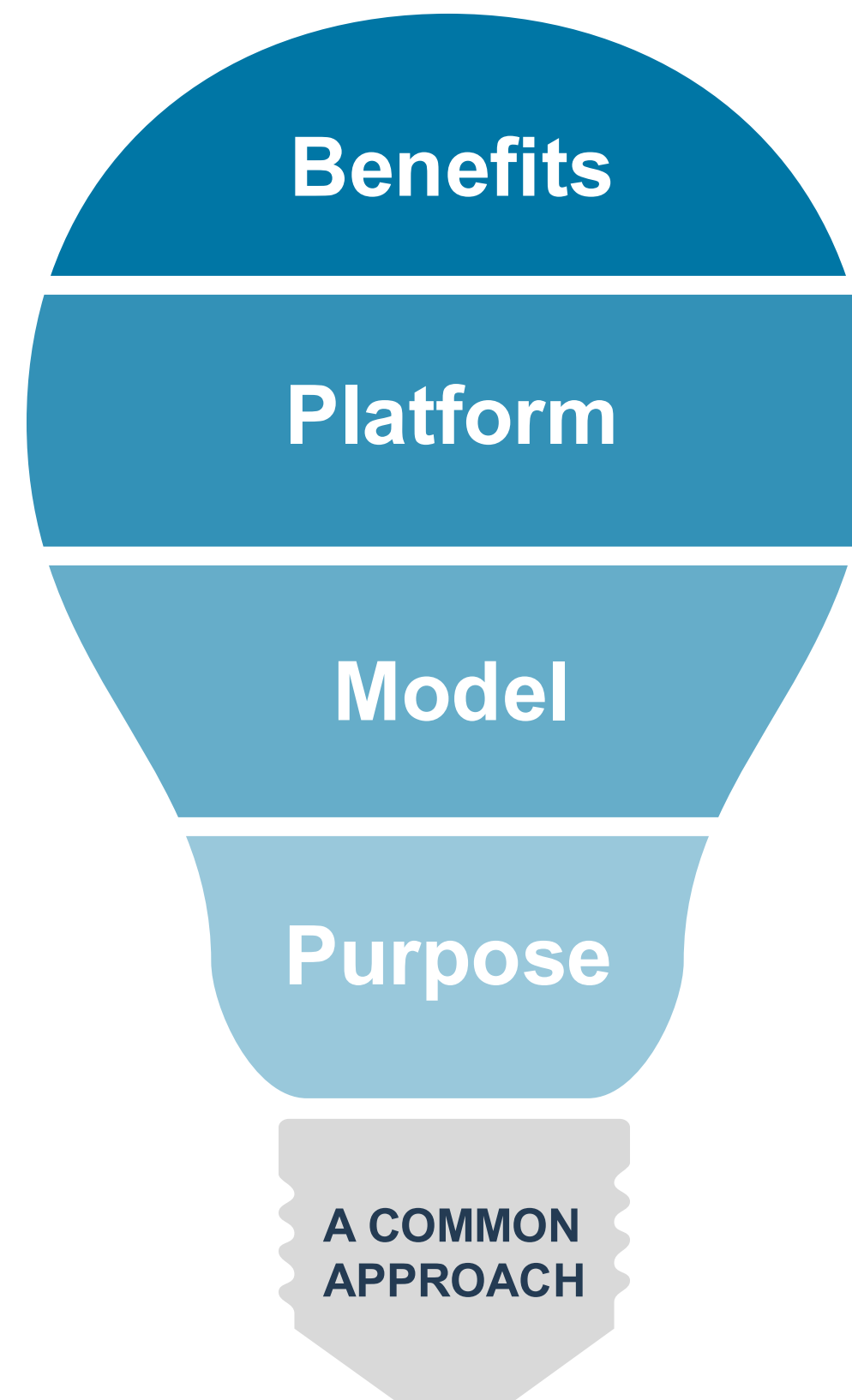
Sharing to Protect: A Common Platform for Cyber Security Lessons

Purpose

Transform incidents, near misses and attacks, whether cyber-related or not, into shared knowledge.

Model

Inspired by IBM X-Force Exchange – shaping action through collective experience.



Platform

Evolution to a Cloud-based threat intelligence platform with anonymized data

Benefits

Faster identification of emerging threats, collective defence and continuous improvement, definition and sharing of best practices

To build trust and resilience across the ferry industry

Conclusions

An Integrated Cyber Risk + Business Continuity Approach



Enables evaluation and management of risks beyond pure cyber security including human factor:

- Information & Awareness
- Training & Drills
- Responsiveness



Ensures operational continuity of the ferry in all dimensions in the entire life-cycle:

- Technical
- Commercial
- Reputational
- Sustainability



Provides a competitive advantage:

- Greater resilience
- Reduced disruption costs
- Protection of passengers and crews

Assets Value Enhancer!

Thank you!



For further info:

Maria Garbarini
Head of Passenger Ships
Excellence Centre
maria.garbarini@rina.org

Danilo Diomede
Certification Cyber & IT Product
Manager
danilo.diomede@rina.org

