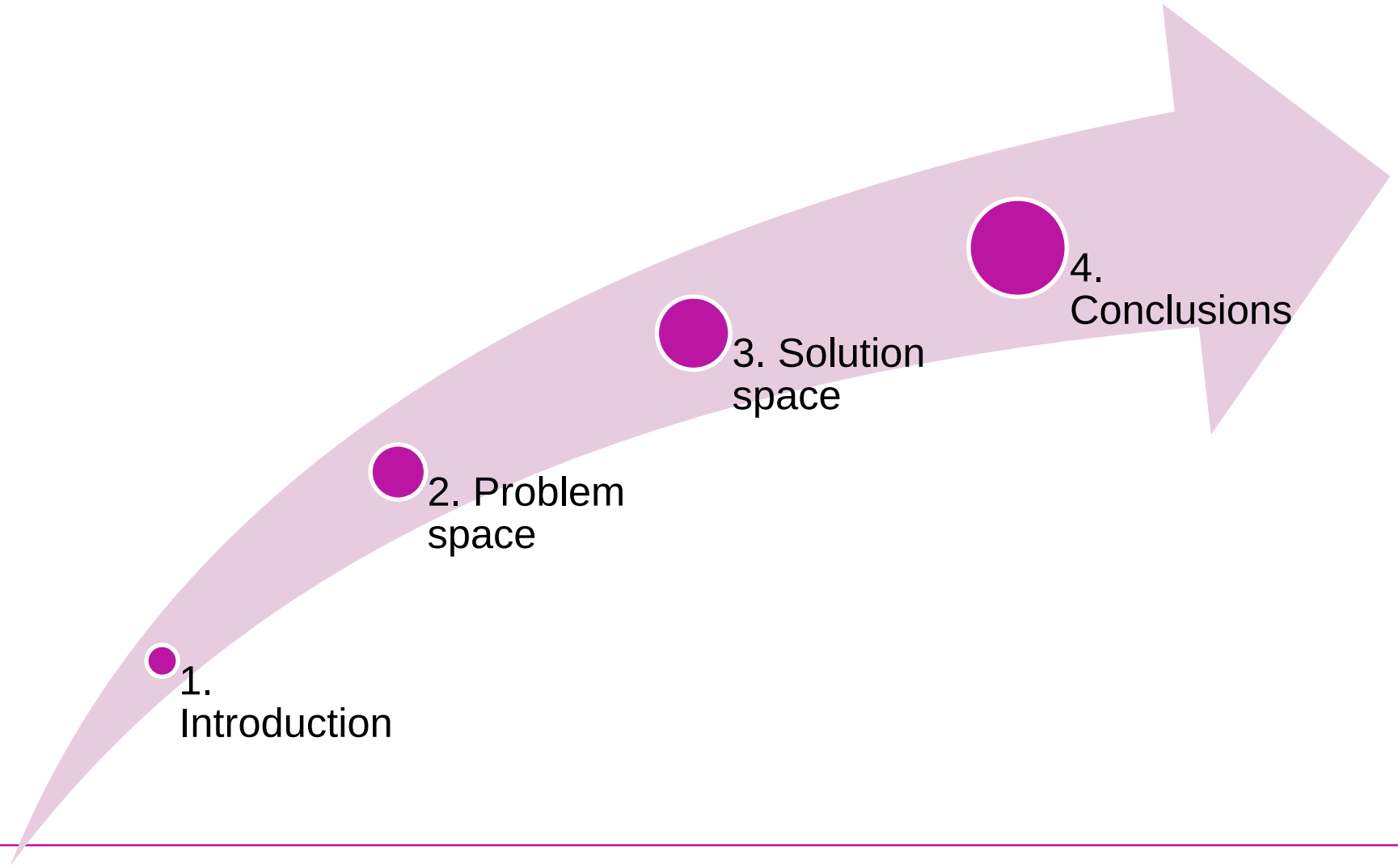
Aalto University
School of Engineering

Cybersecurity risk assessment for autonomous maritime systems – challenges and opportunities

Dr Victor Bolbot
Risks and Intelligence in Marine Systems, Marine Technology Group,
Department of Mechanical Engineering, Aalto University, Finland

17.4.2023

Contents


1. Introduction
2. Problem space
3. Solution space
4. Conclusions

1. Introduction

- **Antikythera mechanism – the oldest example of analogue computer 200BC**
- **First computer – 1942 (ABC) (1947 ENIAC)**
- **1950 – 1980 First attacks, ethical hacking, malware, hacking, legal prosecution**
- **1980 – 2010 Internet, commercial cybersecurity, attack vector growth**
- **2010s – Attack on the industrial control systems including ships**
  - GPS jamming/spoofing (influencing AIS)
  - Malware infections
  - Attacks on oil terminals / infrastructure
  - Attacks on ship operating servers
- **Autonomous ships development**
  - Multiple tests around the globe
  - Japanese car ferry Soleil automatic berthing in 2022
  - Yara Birkeland – autonomous sailing a few days ago

2. The problem space – factors complicating risk assessment

- **Ships**
  - Designed to operate for 25 years < (even more for IWW)
    - *Very long period of time – need for continuous update of systems*
    - *New cyber attacks are being developed and vulnerabilities found*
    - *New phishing attacks using GPT-4*
  - Heterogeneity of ship systems
    - *Both Information Technology (IT) and Operational Technology (OT)*
    - *Use of various systems providers (OT and IT) and problems with integration*
  - Increased connectivity with shore, ports, service providers, infrastructure (locks)
    - *Increased attack vector (more attacks)*
  - Autonomous shipping and decision support systems
    - *More decision-making transferred to control systems*
    - *More need for communication with shore*
    - *Less potential for human intervention*

2. The problem space – factors complicating risk assessment

- **Processes – Organization**
  - Lack of widely and acceptable risk acceptance criteria, risk metrics, scales for ranking and risk assessment processes
    - *Diversity of approaches and opinions*
    - *Difficult comparison and verification*
  - Lack of historical data (can it be useful?)
    - *Underreporting*
    - *Potential future vulnerabilities*
  - Ensure transparency
    - *Collision between safety and cybersecurity*
  - Penetration testing
    - *Software complexity, scalability, mobility*
  - Lack of processes and entities gathering incidents reports
  - Cyber resilience
  - Small companies have limited resource for cyber management

2. The problem space – factors complicating risk assessment

Humans

Lack of cyber skills and hygiene

Lack of standardization of training guidance

Problem with situation awareness

Cyber resilience training

Environment

Change of ownership

- Legacy systems

International nature

- Difficult to come to agreement with respect to regulations and technical solutions

Covid 19, international turmoil due to Ukraine

Safety risks

Multiple attacker groups

2. The problem space – factors complicating risk assessment

	Minor consequences	Severe consequences
Highly likely	Attacks on IT services	
Low likelihood		Attacks on OT services

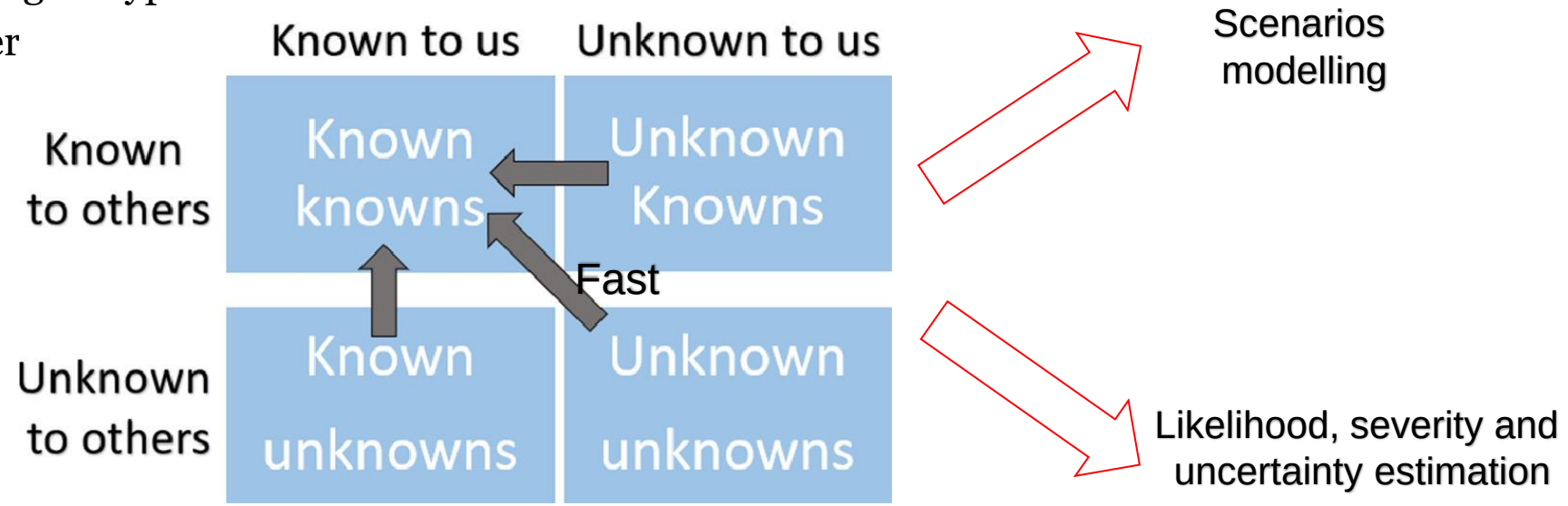
The situation is dynamic

Perrow – Normal Accident Theory
The importance of low likelihood but high severity accidents
The possibility of black swans
Different in autonomous ships

Speed 2: Cruise control
Film launched in 1997

3. The solution space

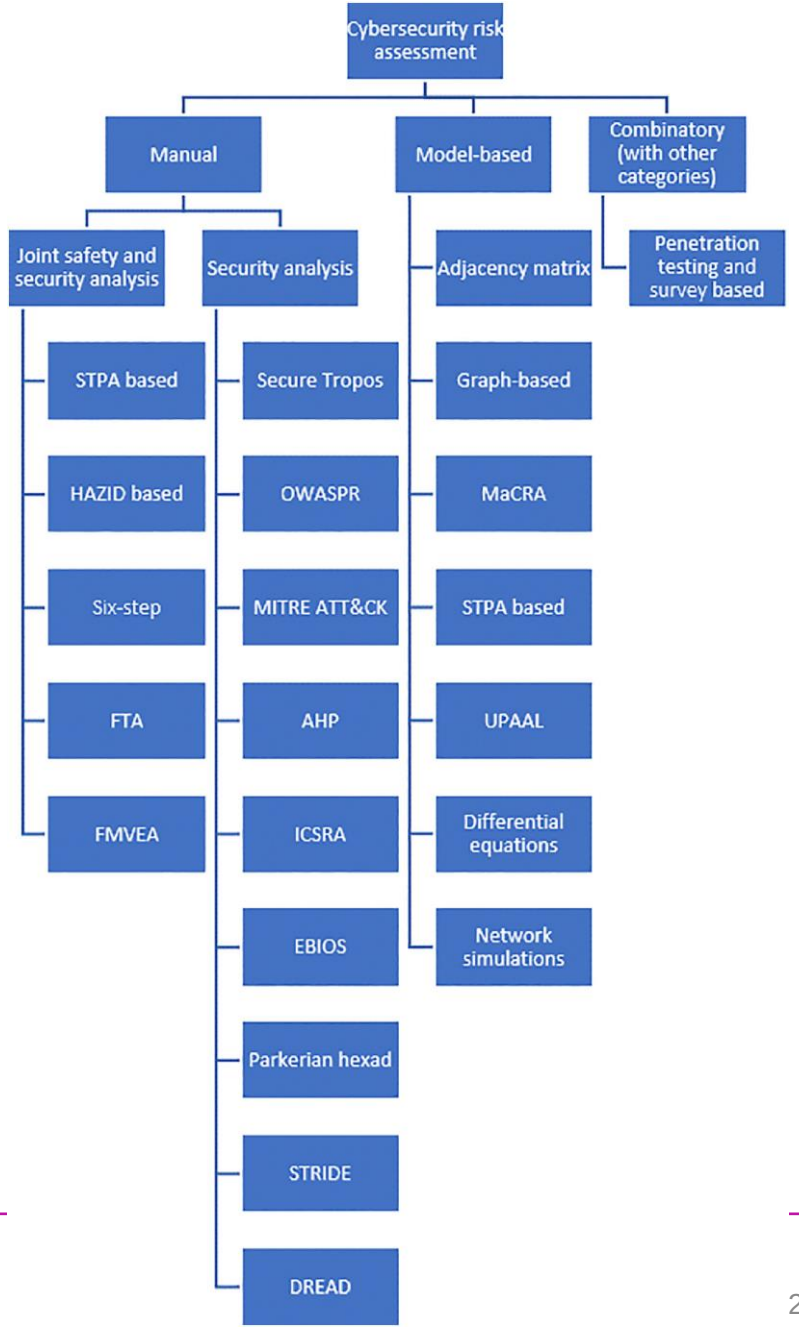
- **Most of the challenges can be easily solved (Pareto rule 20-80)**
- **Addressing of the unknown dynamically**
  - Novel organizational approach to fixing the vulnerabilities
  - Considering the emergent types of vulnerabilities
  - The sooner the better



3. The solution space

Dr Victor Bolbot, Dr Ketki Kulkarni, Ms. Päivi Brunou, Prof. Osiris V. Banda, Prof. Mashrura Musharraf, 2022, “Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis”

- Analysis of Scopus-based studies
- Safety based
- Security analysis
- Model-based
- Combinatory



3. The solution space

STPA is very popular in safety engineering for MASS
- Pros – Emergent scenarios, social structure, attack propagation modelling
- Cons – Too complex and resource intensive, not directly for cybersecurity problem

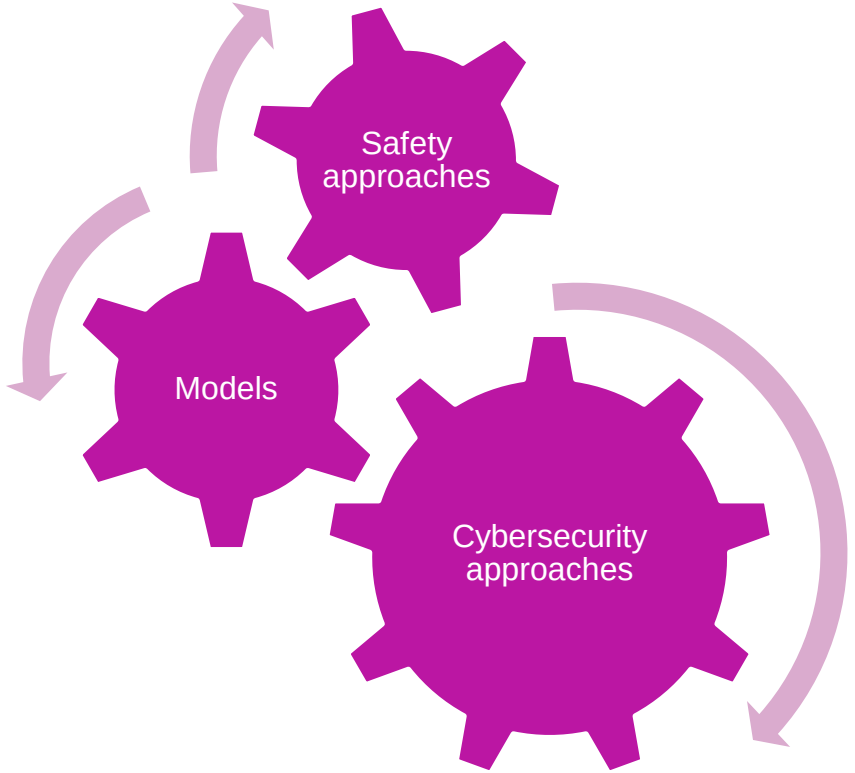
STRIDE, DREAD, OWASP
- Pros – Simple, well-known,
- Cons – Captures the basic events, not the emergent

FMVEA, HAZID
- Pros – good for capturing effects of attacks in OT systems
- Cons – Not for identifying propagation of attack, not for emergent phenomena

FTA, Attack trees, MITRE ATT&CK, Secure Tropos
- Pros – modelling complex scenarios
- Cons – resource intensive

- **Based on the experience of personnel**
- **Difficult to update in case of new vulnerabilities**
- **Good for understanding the modeling requirements**
- **Novel risk types**
- **Good for reporting**

Model – based approaches
- Pros – Easier to reassess
- Cons – Selection of proper abstraction and interconnection to the other methods

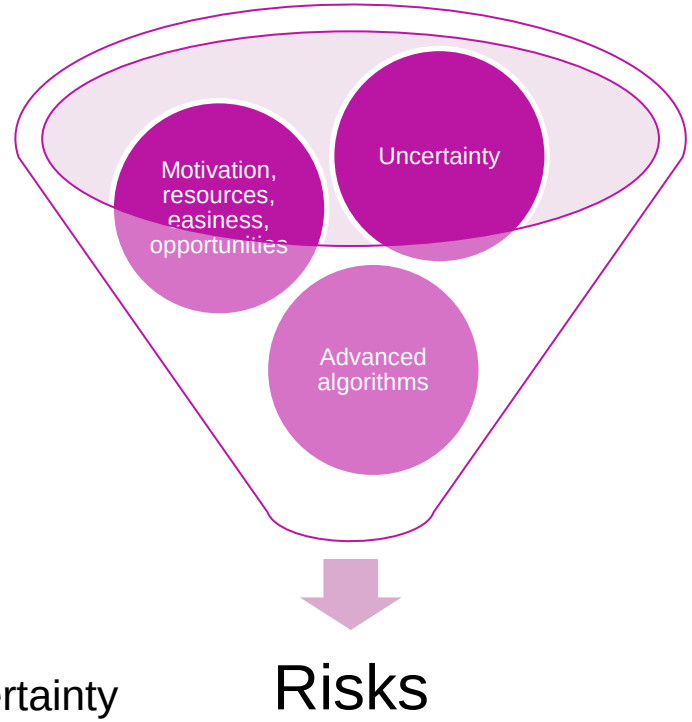


3. The solution space

Platform for reporting of anonymized incidences

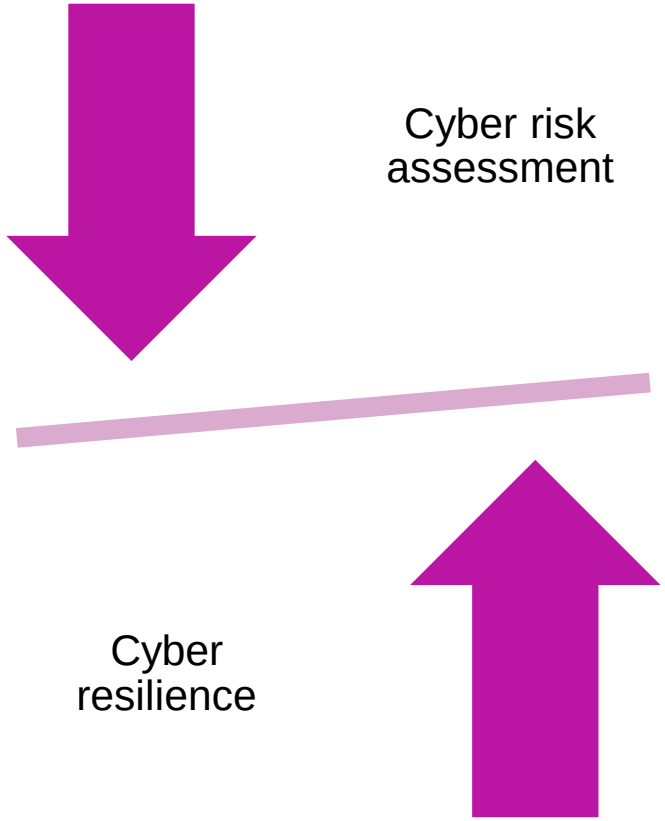
- We can learn a lot from accidents
- Important to disseminate the learning outcomes
- Good foundation for risk assessment an

- **Relying on historical data is not a sole solution due to black swans**
  - Problem of induction
  - Too many reports
- **Most of the risk assessments method considered**
  - Motivation
  - Resources
  - Easiness
  - Opportunities
- **More advanced methods could include**
  - Epistemic (system unknown) and aleatory (variation in known parameters) uncertainty
  - Game theory
  - Prey-predator algorithms
  - Immune system response algorithms
  - Real-time update



3. The solution space

- **Plans for cyber resilience management**
  - Ok, we got hacked, what now?
  - Not allowing yourself to get hacked twice
  - Ability to handle the surprise
    - *The importance of uncertainty and slack – Better safe than sorry*
  - Even more in autonomous ships
- **Risk acceptance criteria development**
  - Topic for international collaboration
  - Fundamentals of risk
  - Considering autonomous ships



Conclusions

- **Cybersecurity is a highly dynamic realm with novel attack types being constantly developed**
- **Challenges for the Risk Assessment stem from the ship, processes, humans and environment**
- **IT but also OT ship systems can be hacked**
- **There is an increased need for dynamic risk assessment of cybersecurity**
  - Interconnected and vibrant database of vulnerabilities and attack types
  - New tools for risk assessment and risk management based on models
  - Better consideration of uncertainty and likelihood
  - Greater emphasis on resilience
  - Addressing fundamental risk issues in the maritime

Aalto University
School of Engineering

Thank you for your attention

Dr Victor Bolbot

Risks and Intelligence in Marine Systems, Marine Technology Group,
Department of Mechanical Engineering, Aalto University, Finland

victor.bolbot@aalto.fi