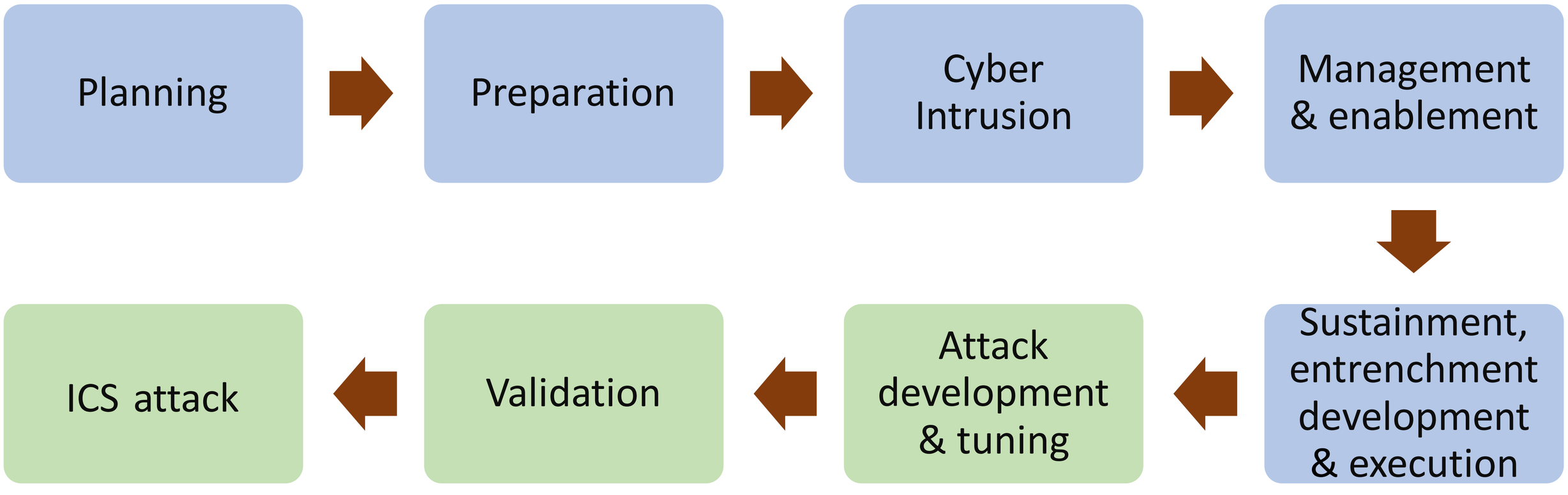
Cascading effects of cyber-attacks on Interconnected Critical Infrastructure

***Motivation**: To investigate attacks on cyber-physical systems, and their cascading effects.*

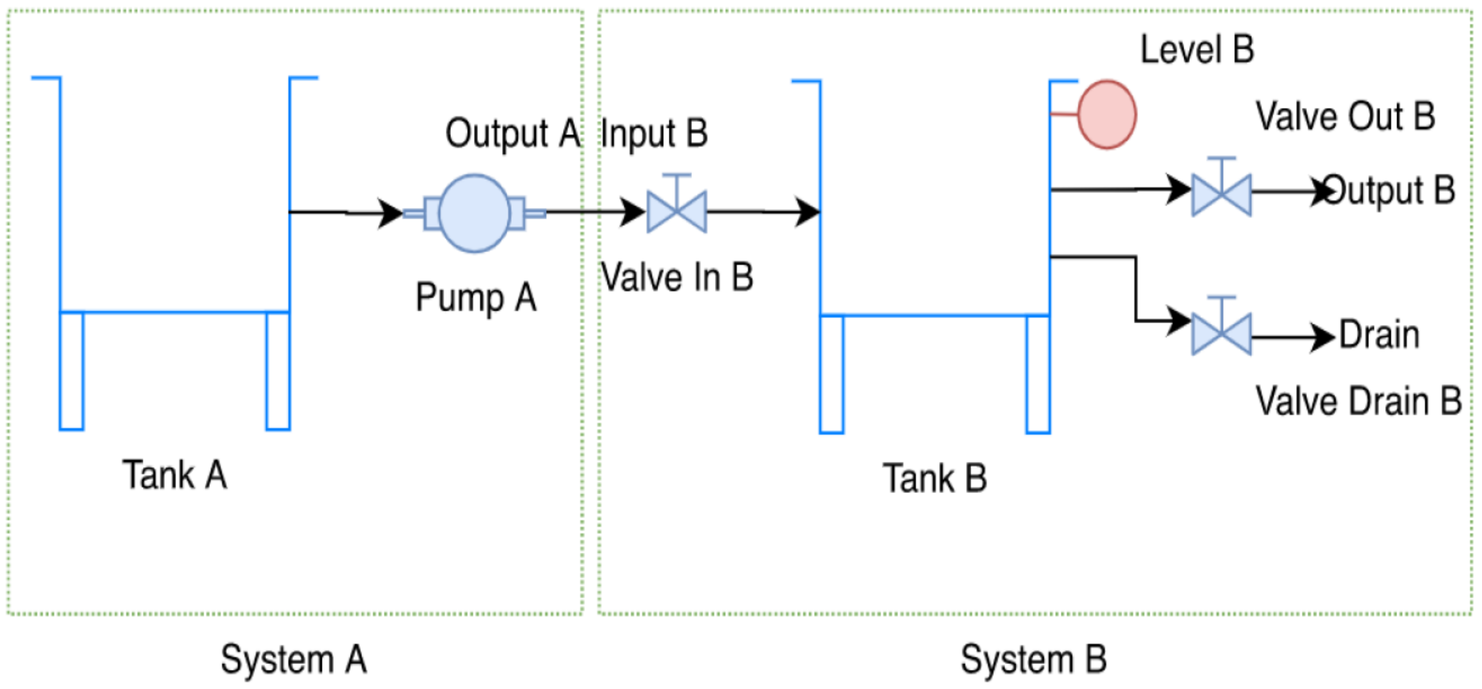
ICS Cyber Kill Chain



Cascading Effects

- Attacks on critical infrastructures are becoming more and more sophisticated.
- **Cascading effects** are caused when a primary incident triggers propagating phenomena to nearby components, causing chaining accidents which lead to an overall result more severe than the initial action.
- Example of draining tank A by opening the valve in B, turning pump A ON and opening valve drain in B.

Example of an interconnected system



Research questions

- What components need to be targeted in order to achieve cascading effects?
- How to automate the attack design even w/o system information.
- How is the system resilience reduced?

Methodology

- Literature review.
- Practical work on testbed.
- Investigation of attacks on CI
- Investigate the resilience of the system.
- Defense and mitigation.

Key advances

- System of systems – a mechanism to conduct impact analysis.
- Attack modelling – a mathematical framework for attack models.
- Prototype tool – Physical design with security analysis.

References:

[1] Michael J Assante and Robert M Lee. “The Industrial control system cyber kill chain” . In: SANS institute InfoSec Reading Room 1 (2015).

[2] Venkata Reddy Palleti et al. “Cascading effects of cyber-attacks on interconnected critical infrastructure” . In: ACM SIGMETRICS Performance evaluation Review 47.4 (2020).

Marios Samanis marios.samanis@bristol.ac.uk
Sridhar Adepu adepu_Sridhar@alumni.sutd.edu.sg
Awais Rashid awais.rashid@bristol.ac.uk

University of BRISTOL
Bristol Cyber Security Group