Norwegian Centre for Research-based Innovation

NORCICS

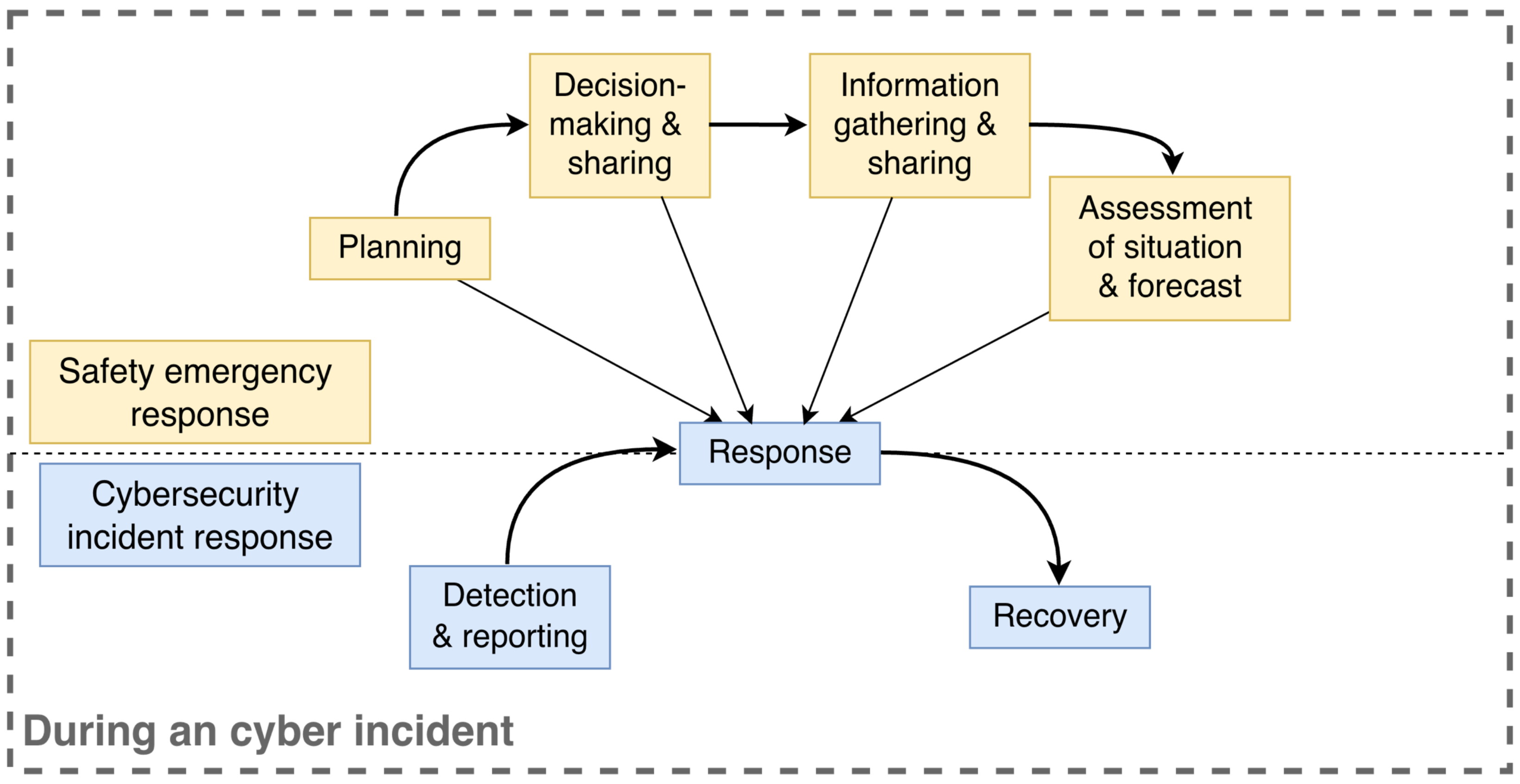
SFI Norwegian Centre for Cybersecurity in Critical Sectors

A model-driven approach to define a joint incident response plan

Visualizing plans considering safety emergency response and cybersecurity incident response during a cyber incident with physical consequences (e.g., hydrocarbon leakage, power outage) can contribute to tabletop exercises, revising the events in a previous cyber attack, resource allocation and preparedness planning between IT security, OT teams, and external actors.

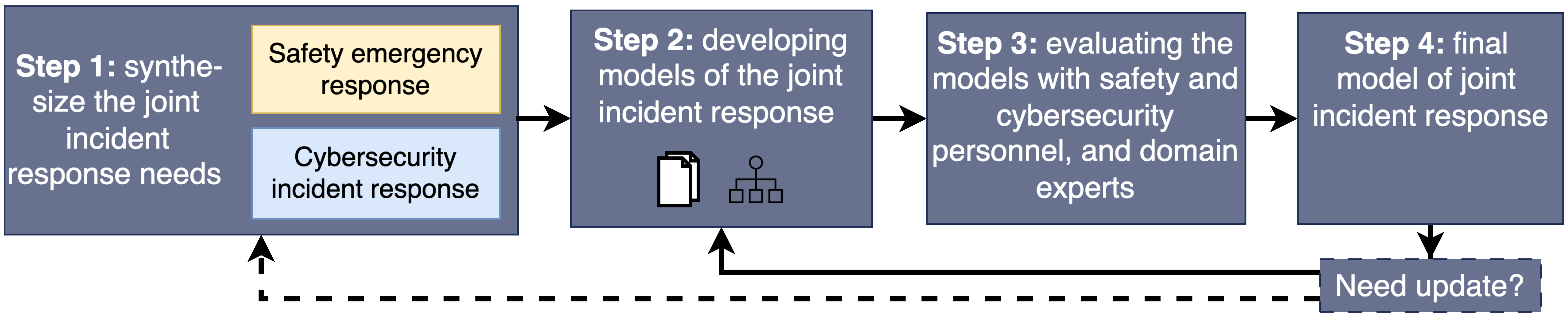
How can the joint incident response plan be represented, so that it is fully understood by all stakeholders?

Joint incident response process


Decision-making & sharing
Information gathering & sharing
Planning
Assessment of situation & forecast
Safety emergency response
Response
Cybersecurity incident response
Detection & reporting
Recovery
During an cyber incident

Adapted from models in ISO 22320, ISO 27035, and NIST SP 800-61r3

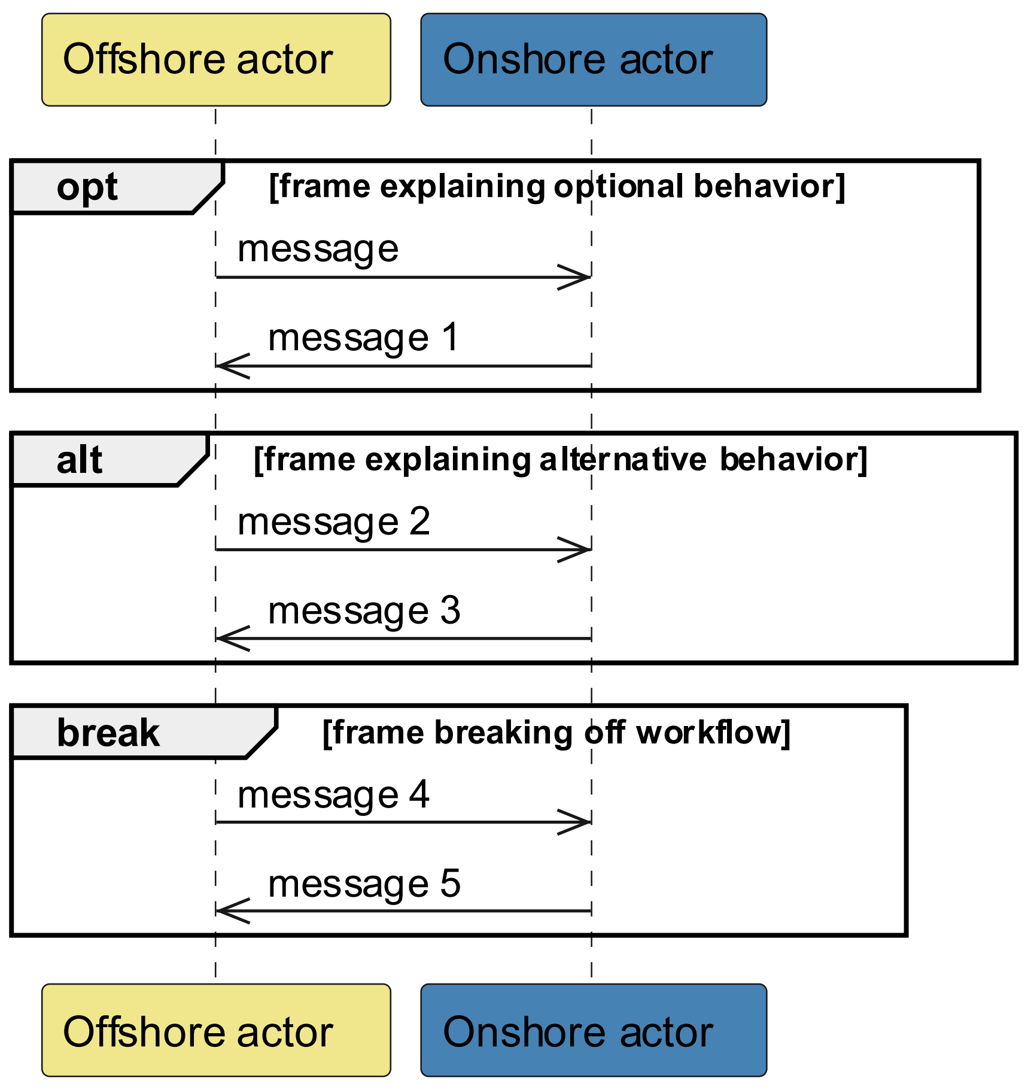
Model-driven framework

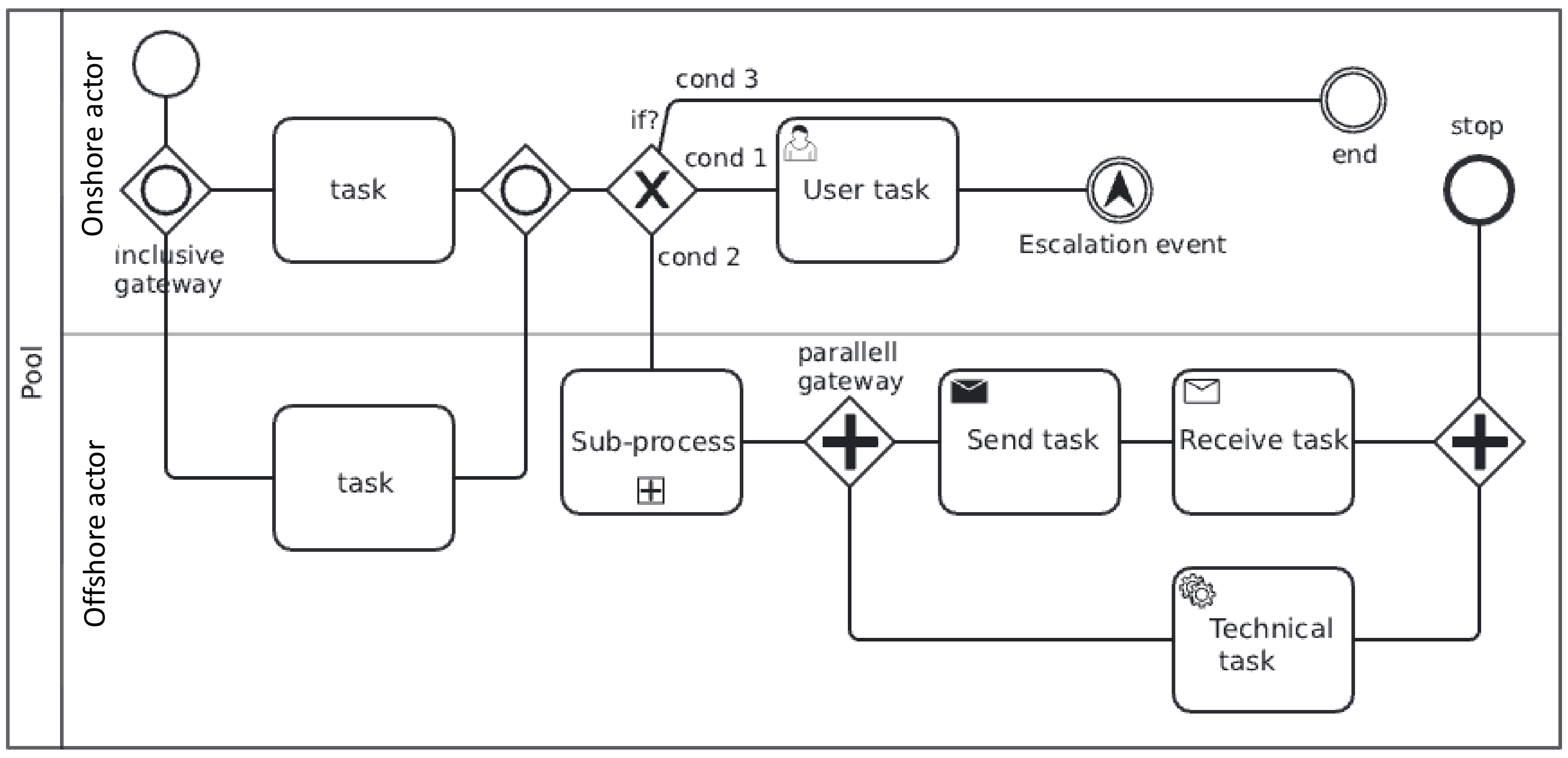

Step 1: synthesize the joint incident response needs
Safety emergency response
Cybersecurity incident response
Step 2: developing models of the joint incident response
Step 3: evaluating the models with safety and cybersecurity personnel, and domain experts
Step 4: final model of joint incident response
Need update?

One way to define joint incident response models is to use UML Sequence or BPMN diagrams.

UML Sequence diagrams focuses on the exchanged *messages* between roles. However, due to the inherent concurrency and number of possible orderings of interactions in the joint incident response, SDs become hard to read for a preparedness plan, but could provide a comprehensive overview when revising and modeling previous cyber attacks.

BPMN diagrams focuses on *tasks* specifically performed by an individual role. BPMN is already utilized in incident response playbooks. Sequence and BPMN diagrams becomes larger as the number of roles (e.g., lifelines, lanes) increases, making it more complex in terms of readability.





Vahiny Gnanasekaran
PhD Candidate
NTNU & SINTEF Digital

More detailed examples from these and other diagram types can be found in the DataverseNO repository.