Company Restricted

COMBITECH

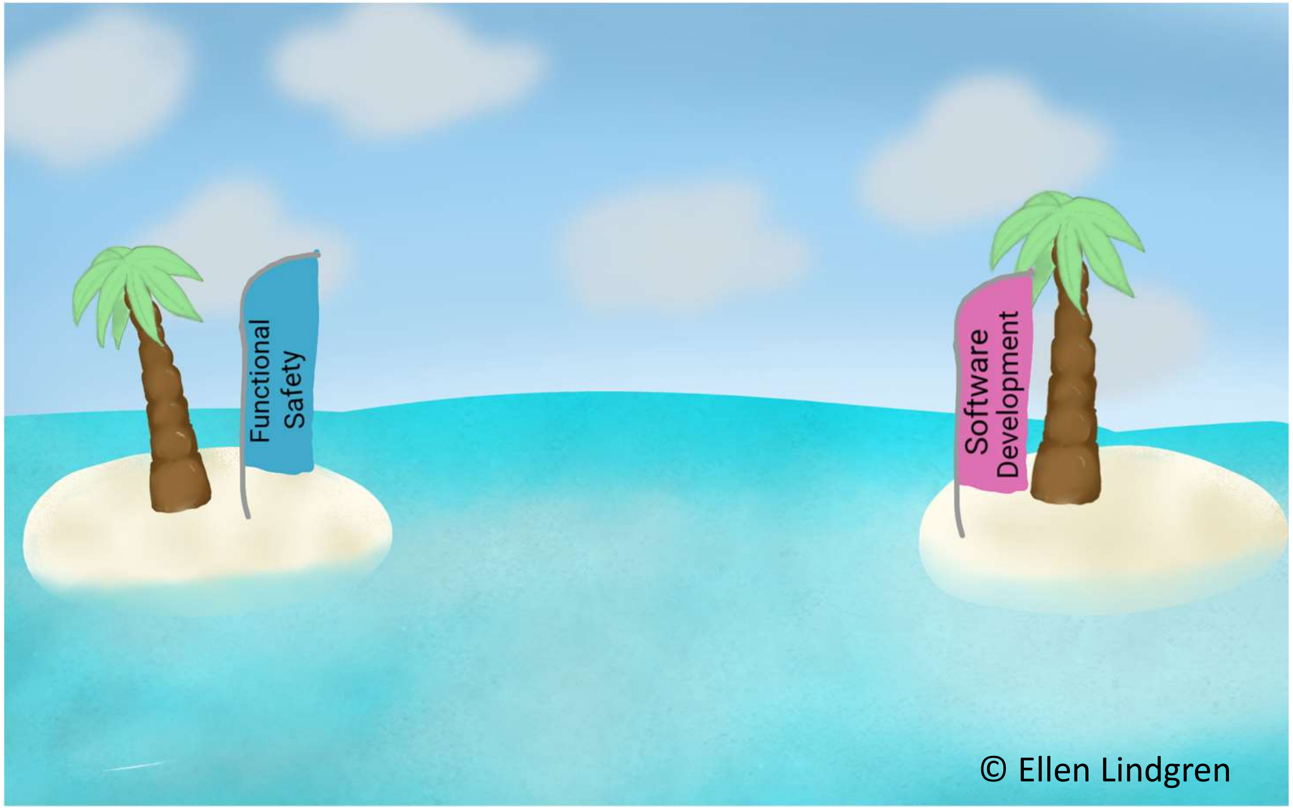
BRIDGING THE GAP BETWEEN FUNCTIONAL SAFETY AND SOFTWARE DEVELOPMENT FOR SAFETY CRITICAL SYSTEMS

Presentation on 9th Scandinavian Conference on System and Software Safety, November 23-24 2021

Mattias Lindgren

System Safety Consultant

SETTING THE SCENE – THE GAP



© Ellen Lindgren

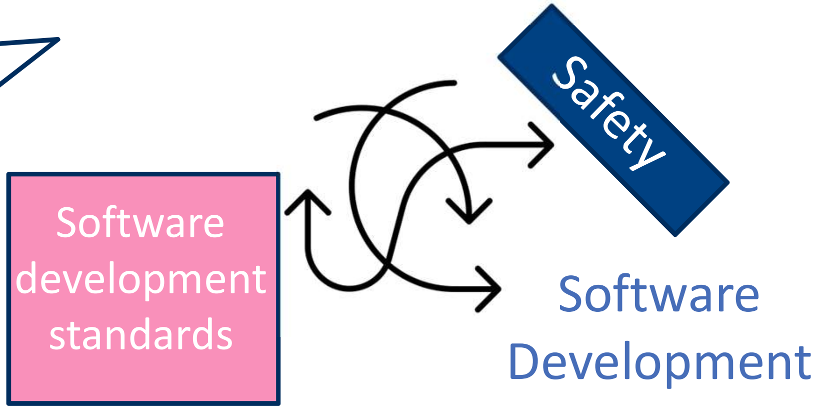
DEMYSTIFY SOFTWARE SAFETY

Establish Development Assurance principles

Need for interpretation and tailoring

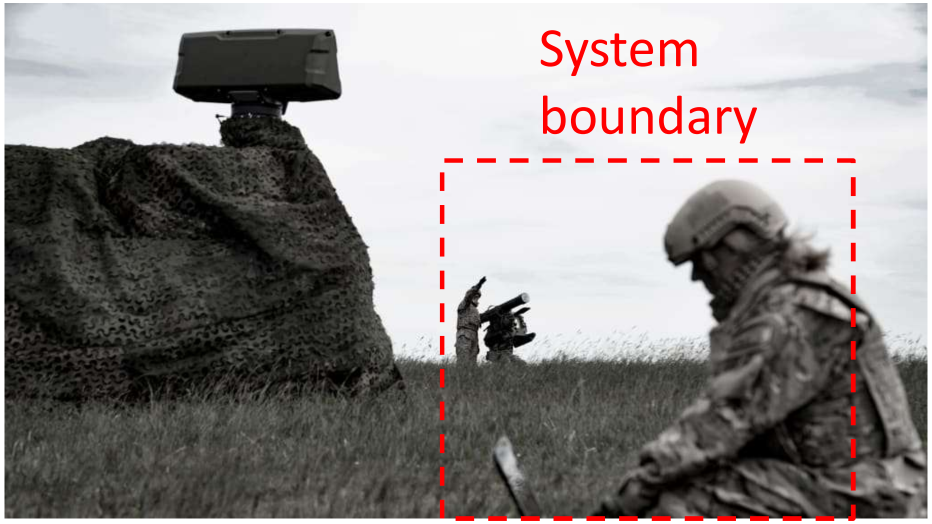
Integrate the intent of the standard in software development processes

Avoid uncertainties – clear decisions on new way of working



EARLY FUNCTIONAL SAFETY ASSESSMENTS

- Establish a methodology for functional safety assessments.
- Perform Functional Safety Assessments early in a project, with stakeholder participation.
- Develop a common understanding of the accident risks, functional safety drivers and mitigations external to the system.



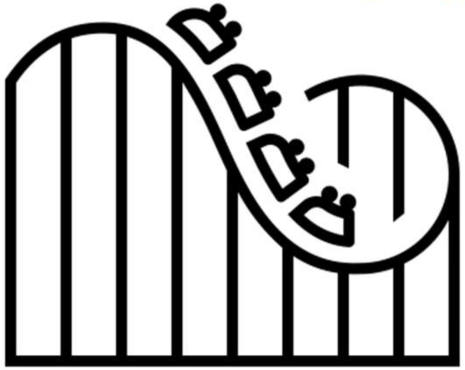
Source: Saab.

MANAGING A HOLISTIC SAFETY VIEW OF THE SYSTEM

Develop with iterations and prepare for changes.

Design for safety - incorporate risk mitigations in system design

.



Managing requirements –correct requirements are essential for software safety

System Safety – a common objective

CROSS-DISCIPLINE COLLABORATION

- Train disciplines of the fundamentals for the other disciplines work
- Define activities when collaboration is needed
  - Documents production/reviews
  - Management of changes.
- Report on on-going work
  - Identifying issues that needs to be discussed with cross-discipline impact.
  - Avoid incorrect interpretations.
- Safety Control Board with key stakeholders– resolve issues.

PROACTIVITY AND PLANNING

~~REACTIVE~~ PROACTIVE

✓Ensure planning of all work to be performed due to the standards applied.

✓Clarify project scope and outcomes, avoiding different interpretations (what, how, when, who).

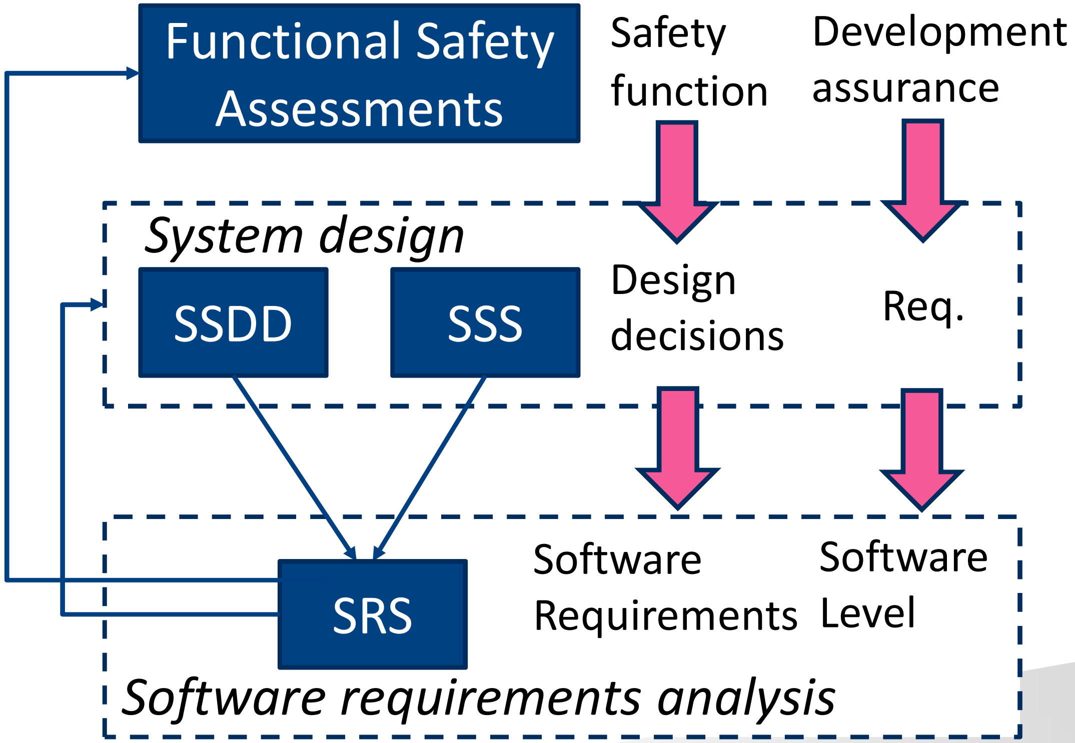
✓ Interpretation of requirements and which document to prove requirements fulfillment.

✓A system supplier should be able to present a statement regarding the software assurance process implemented for a product, e.g. applied standard and software level.

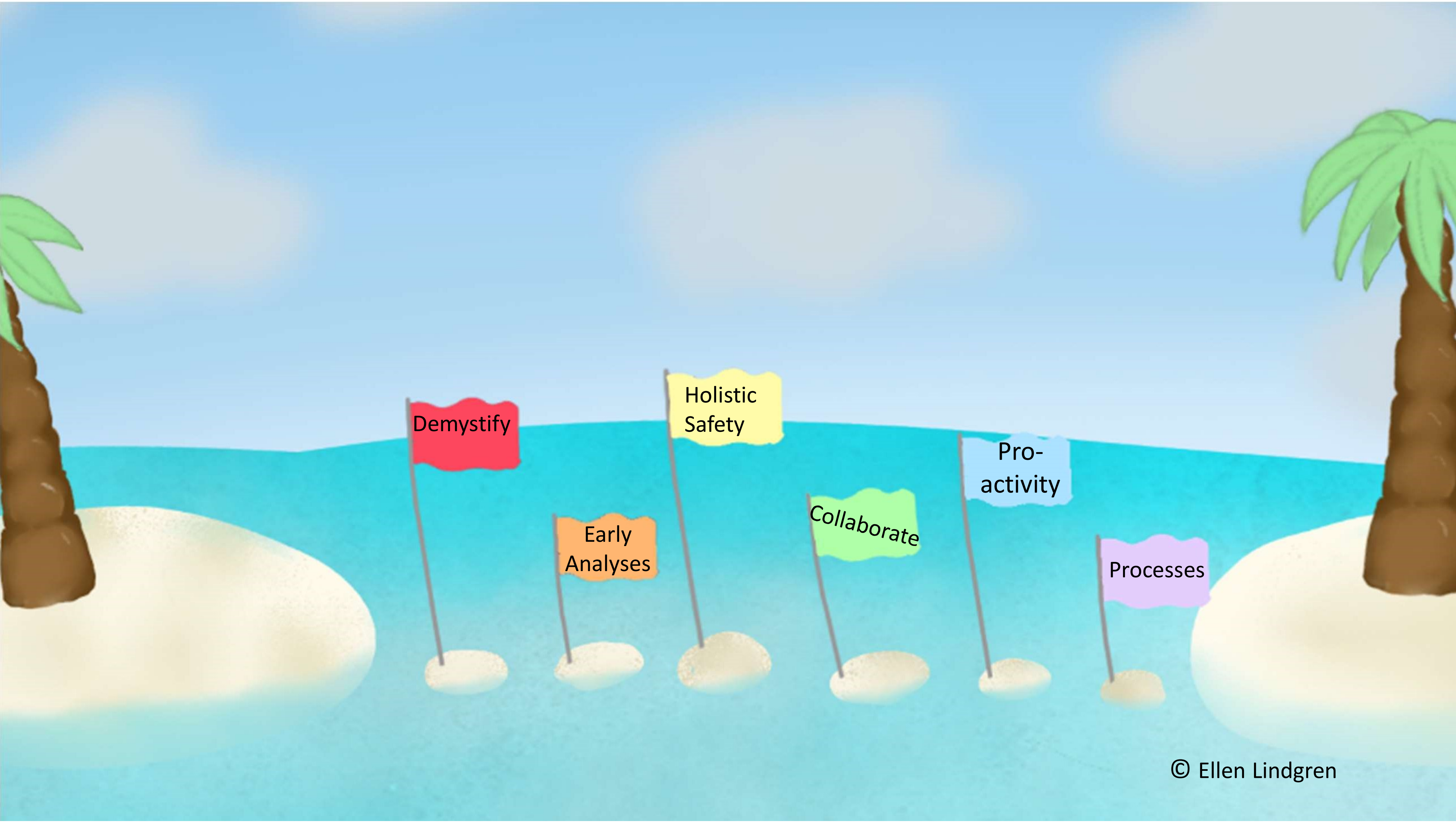
COMBITECH

DEVELOP PROCESSES, TRAINING AND SHARE LESSONS LEARNED

- Develop processes covering information flow from system level work (including safety assessments) to software development.
  - Define interrelations between documents, inputs-outputs.
  - Documents production, content and technical reviews.
- Perform training throughout the organization.
- Use lessons learned as a tool for improvements and make experience part of company processes.



COMBITECH



© Ellen Lindgren

COMBITECH