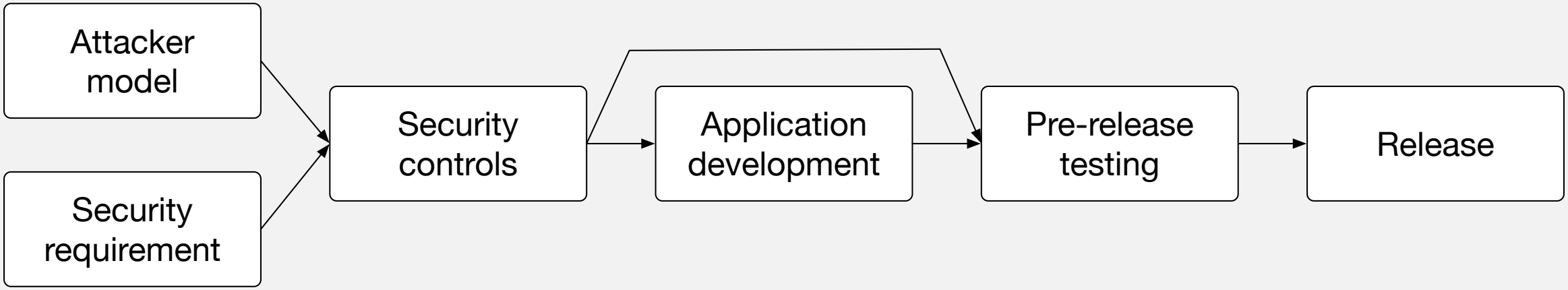
Threat surface analysis as a versatile tool for deciding on cybersecurity measures

Dan Bogdanov, PhD Chief Scientific Officer SAFEST workshop, June 19th

CYBERNETICA

Security and privacy engineering process

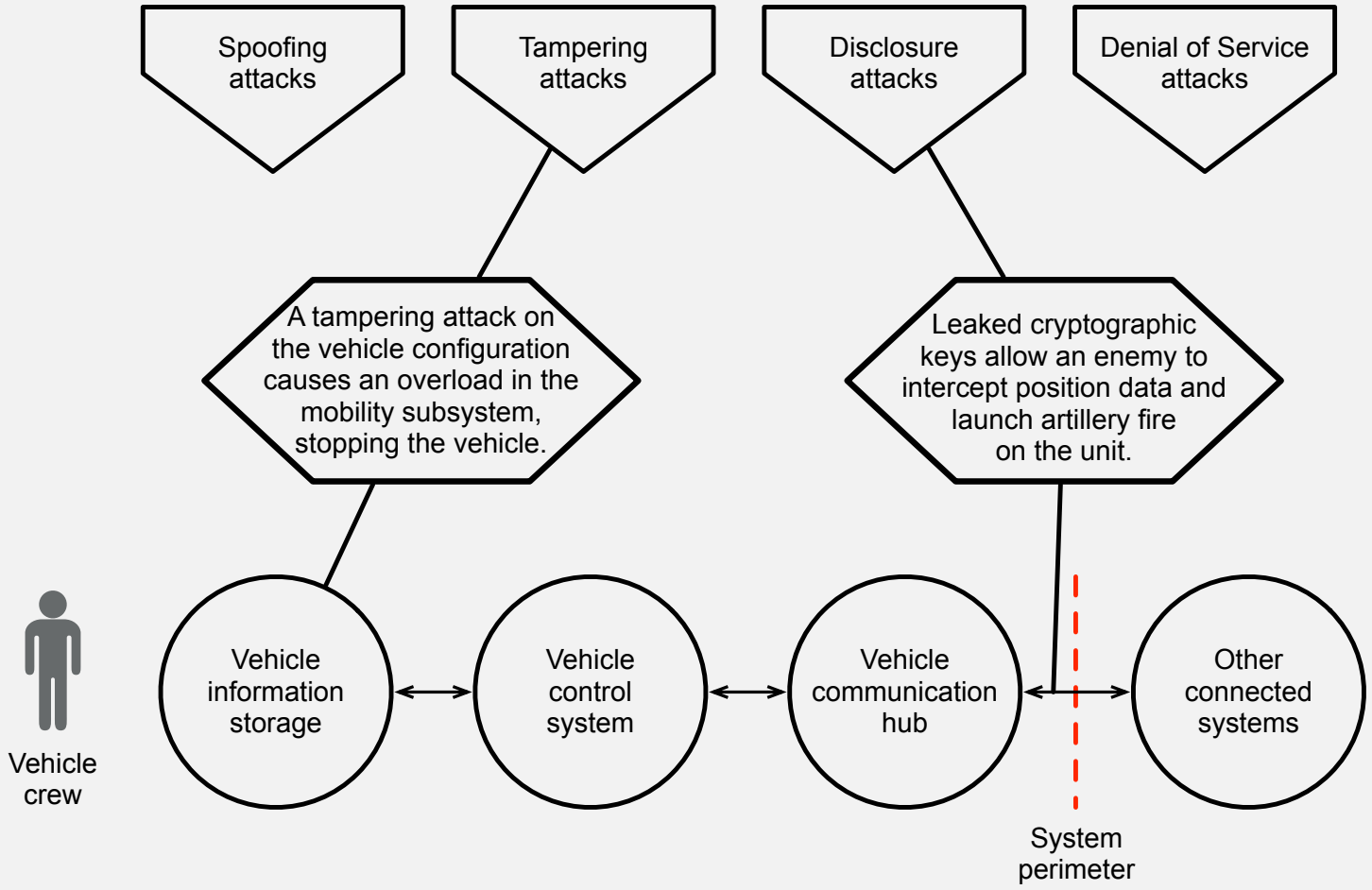


Systematically combine threats and the system

Threat categories

Threat catalogue

Threat surface

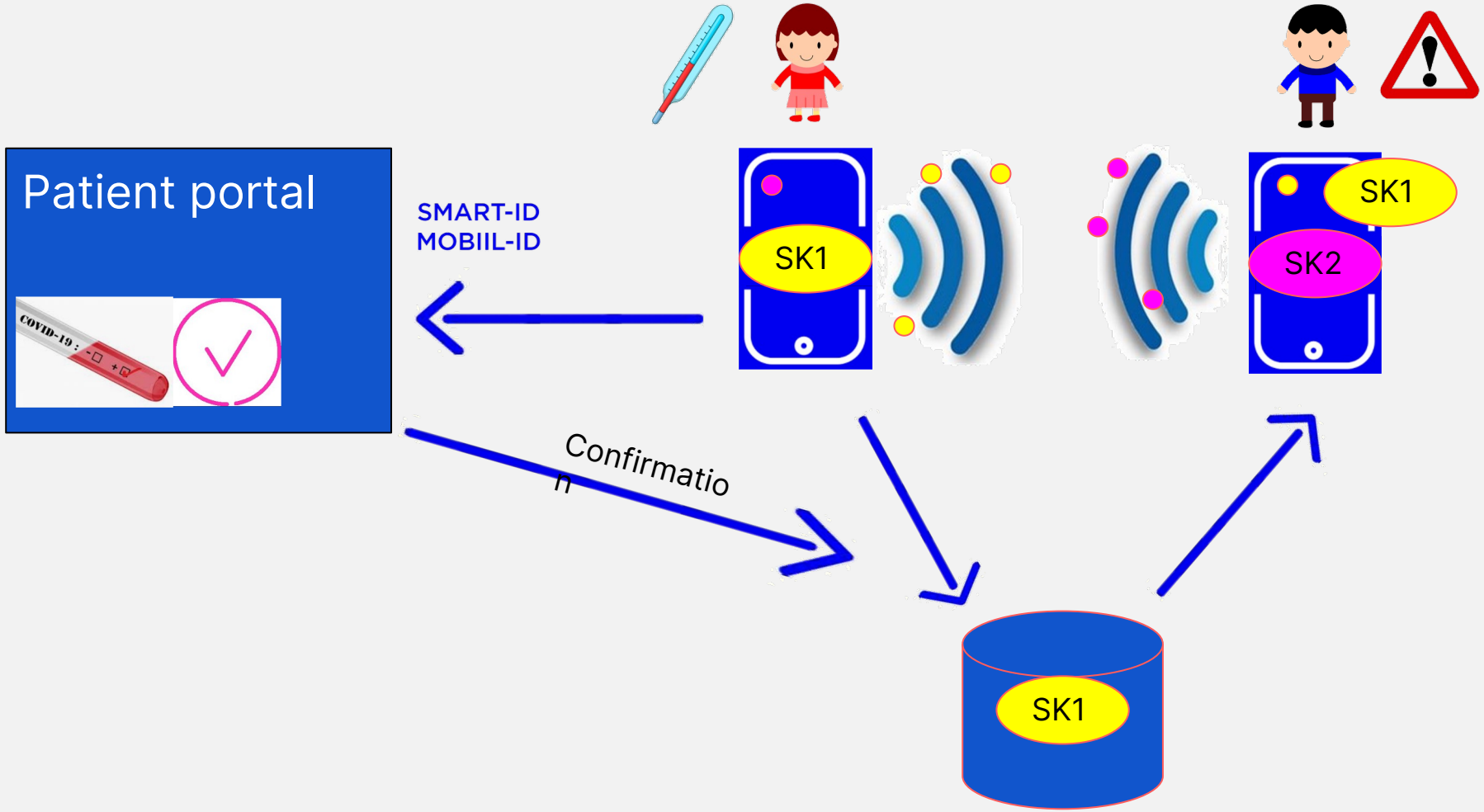


The threat catalogue helps the design systematically identify vulnerable components and select controls and technologies to counter the threat.

Methodology and benefits

- **A disciplined methodology**. A clear analysis structure avoids duplicate threats and, thus, duplicate countemeasures, reducing costs.
- **Keep track of justifications of security measures.** For each control or countermeasure, there is a link back to the original requirement and threat that it is countering.
- **Cost optimisation support**. The model lets you check if multiple controls counter the same threat for the same attack surface. Following an impact analysis, needless countermeasures can be removed.
- **Compatibility with standards and methodologies.** Every step in the analysis can be tagged for relations with other in-house or standardised methodology for compliance.

HOIA – the Estonian COVID-19 contact tracing app

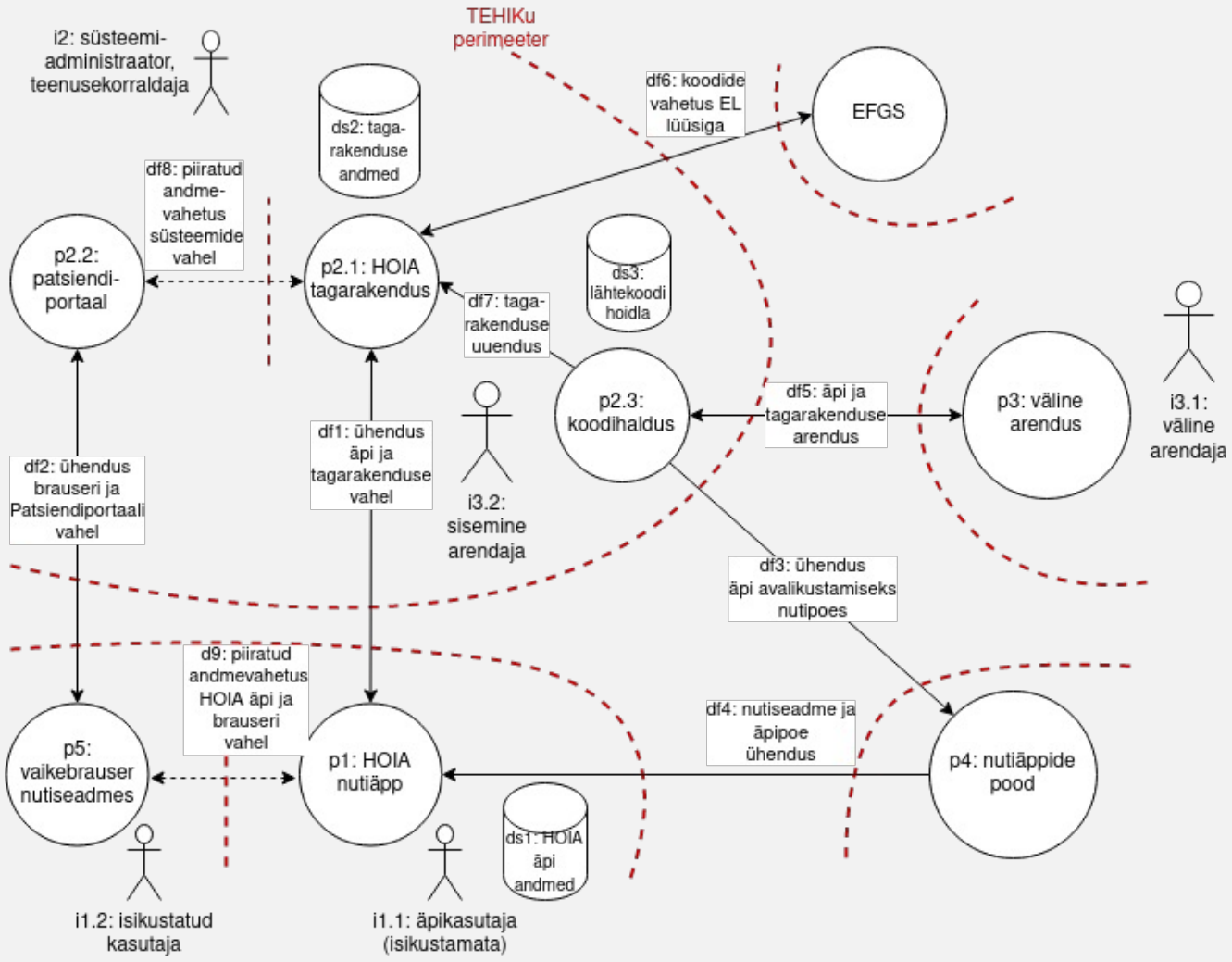


CYBERNETICA

How HOIA was developed

- A consortium of 12 companies set up Slack channels, daily standup calls and joint repositories to start development.
- TEHIK as the operator of most Estonian healthcare IT systems set up wikis, git repositories and deployment environments.
- Several other partners helped with certain jobs (translations, penetration testing)
- All the code and documentation was made available under the EUPL.
  - https://koodivaramu.eesti.ee/tehik/hoia
  - This includes the security analysis and security testing

Attacker model – attack surfaces



- Figure from HOIA documentation (https://koodivaramu.eesti.ee/tehik/hoia/documentation)

CYBERNETICA

Attacker model – threat catalogue

- The threat catalogue has five categories
  - OR – threats from attacks against the app and its users
  - OS – threats from attacks against communications channels
  - OT – threats from attacks against the backend
  - OA – threats from attacks against the development team
  - OP – threats from attacks against user privacy
- The Estonian language document is here: https://koodivaramu.eesti.ee/tehik/hoia/documentation/-/blob/master/ründaja-mudel.md (partially based on DP-3T analysis)

Security requirements

- Two groups of requirements
  - Estonian e-government principles
  - Requirements from ENISA's Cybersecurity requirements and testing for COVID-19 apps report

- The Estonian language document is here: https://koodivaramu.eesti.ee/tehik/hoia/documentation/-/blob/master/turvanõuded.md

Security controls

- Five groups of controls:
  - MO – organisational controls (who delivers, PR, management, etc)
  - MU – universal technical controls (secure channels, cryptography)
  - MR – measures in the phone app (authentication, minimisation etc)
  - MT – measures in the service (input validation, hosting policies etc)
  - MA – measures in the development environment (access control, etc)
- The Estonian language document is here: https://koodivaramu.eesti.ee/tehik/hoia/documentation/-/blob/master/turvameetmed.md

Security audit methodology

- For each control and each requirement
  - Assign responsibility (who needs to make sure it is tested)
  - Decide how to test adherence (requirement satisfied, implemented?)
  - Perform testing, write down who tested what
- Publish report.
- For next releases, we will test changed parts.
- The Estonian language document for the initial release is here: https://koodivaramu.eesti.ee/tehik/hoia/documentation/-/blob/master/hoia-turvaülevaade-august-2020.md

May your systems be secure

cybernetica

CyberneticaAS

cybernetica_ee

Cybernetica

CYBERNETICA