

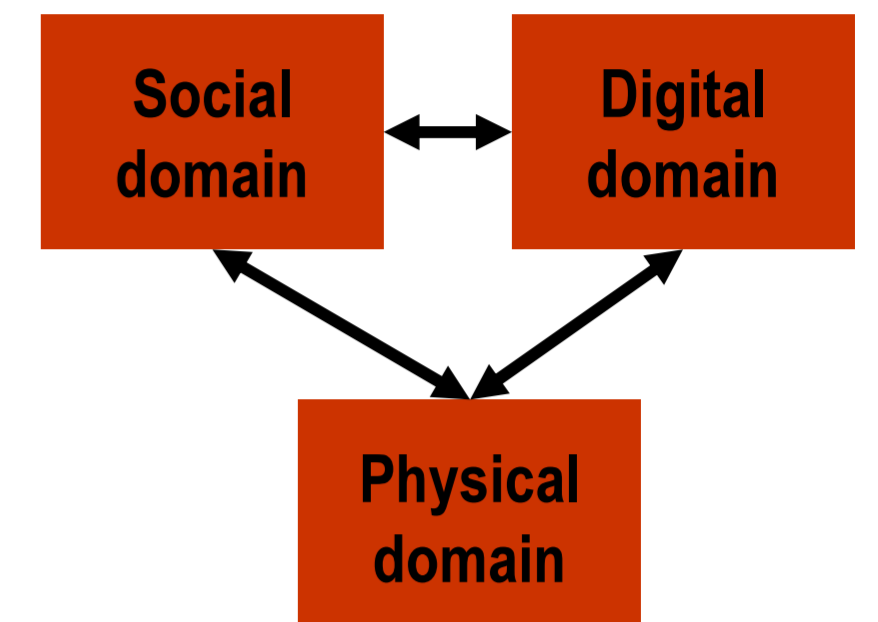


The Virtual Security PERimeter for digital, physical, and organisational security

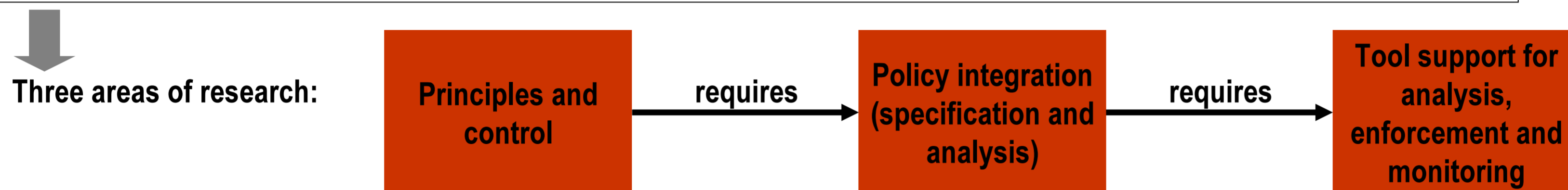
VISPER

A Sentinels research project

The security perimeter, which once was simply defined as the fence around the premises of an organisation, is becoming increasingly flexible and adaptable to the environment and the circumstances. We call this process re-perimeterisation (ReP). The effects of ReP are felt in the digital domain (where data moves from organisation to organisation through networks), the social domain (where one individual may play a variety of roles in cooperating organisations) and the physical domain (where appliances such as mobile phones and laptops move around). In VISPER, we view ReP as managing alignment between these three domains.



In VISPER, we develop methodological and experimental tool support for the specification and analysis of security policies that are integrated across the social, digital and physical domain, as well as security mechanisms that link these domains.



Principles & control

Policy integration

Tool support

Research questions

- Are existing control principles extensible to integrated policies?
- Are there additional principles?
- How do we take mobility into account?

Expected results

Guidelines for applying control principles and security patterns such that mobility and re-perimeterisation are taken into account (e.g., location-based access control).

Research questions

- Which semantic structures can be used to represent the three domains?
- Which rationality constraints across domains have to be imposed?

Expected results

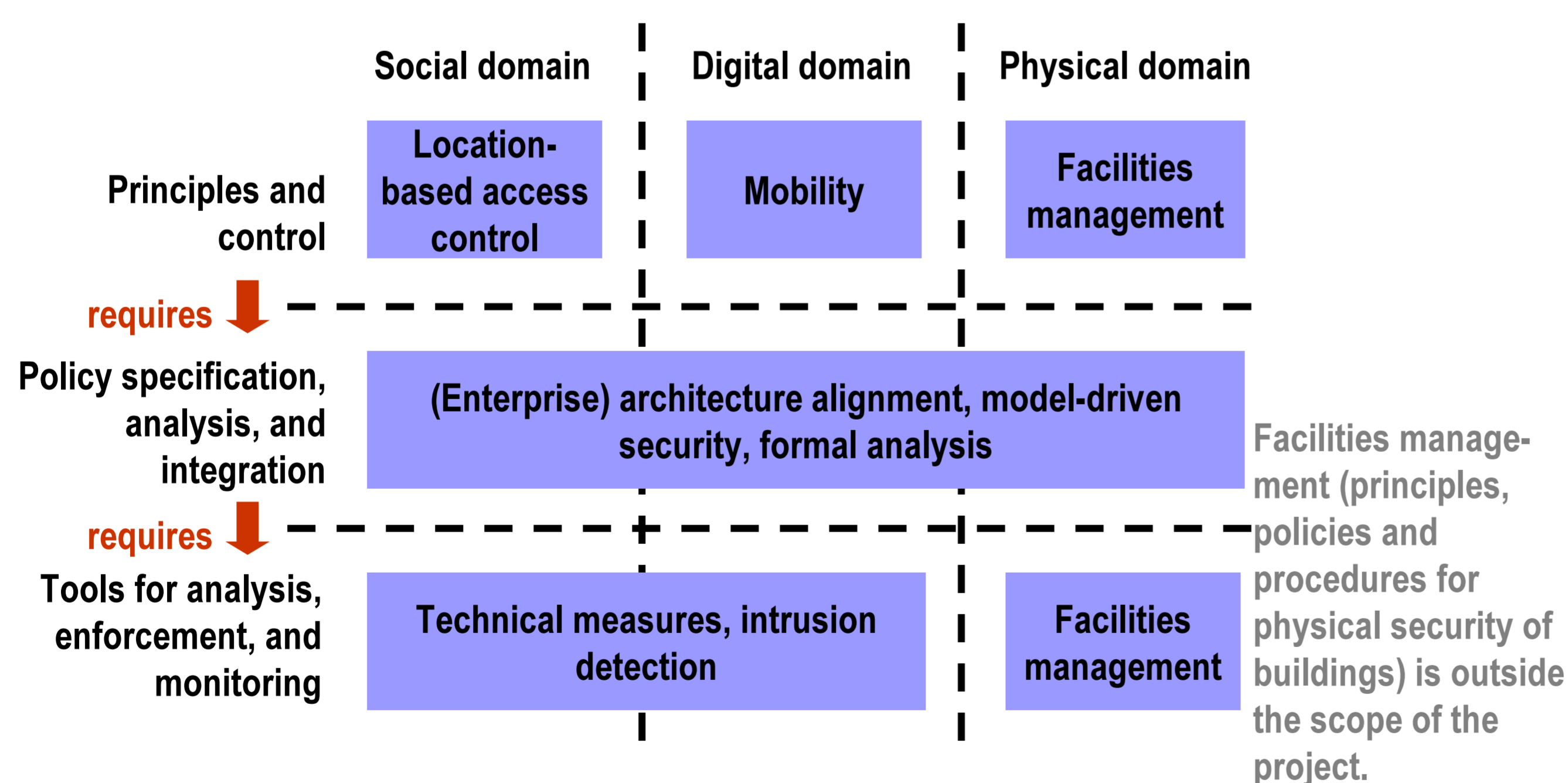
Techniques (methods) for representation (preferably in a formal way) and analysis of IT security policies that are integrated across the three domains.

Research questions

- How to outsource storage of confidential data in a secure way?
- Can tools and techniques from the area of smart surroundings be used?

Expected results

Tools for analysis, enforcement and monitoring.



Application areas

Benign scenarios

- Outsourcing
- Virtual enterprises
- Supply chain integration

Malicious scenarios

- Prevent usage of data on stolen devices
- Manage access to company data for field service employees in 'hostile' environments

Project participants and contact information

Project leader: prof.dr. P.H. (Pieter) Hartel, Distributed and Embedded Systems Group, University of Twente.

<http://visper.ewi.utwente.nl>

Industrial partners: AtosOrigin, the Dutch Tax and Customs Authority, Fox-IT, GetronicsPinkRoccade and BiZZdesign