Management Summary (ENG)

Securing the Vital Infrastructure in the Netherlands is of great importance. If vital facilities are vulnerable, society suffers. Security-by-Design is necessary to be able to approach system security proactively. Here, we study the security of operational technology (OT) including industrial control systems. This technology ensures the monitoring and control of vital infrastructural facilities. In vital infrastructure, the user group is broad and varied. This makes security issues complex and wicked, as they remain unstructured.

The people-oriented Design Thinking design approach focuses on the perspectives of user groups and stakeholders. In this explorative WODC study in response to a request from the National Cyber Security Centre NCSC, it is investigated whether and how the Design Thinking approach can provide added value in the design of solutions for these complex security problems. This has been investigated step by step.

For reasons of security confidentiality, representatives of vital facilities could only offer limited disclosure here. That is why the multidisciplinary research team also consulted scientists, technicians, advisors, regulators, ethical hackers and security officers from a wider circle and a wide range of publications was considered.
The description of the state of security that arises, results in a number of interim conclusions as a prelude to answering the main question: The inventory shows that perfect technical security is not always possible. To design facilities in such a way that they function resiliently in practice, attention must also be paid to the organization of processes and the perspectives of people dealing with the system. This people-oriented appeal offers room for the use of Design Thinking in infrastructure security.

Whether Design Thinking can function and offer added value in practice for infrastructural security issues is also an organisational question. On the basis of a historical overview of Design Thinking and application examples from urban planning, military operations, and transportation safety, and logistics, the main characteristics for Design Thinking in the security context have been formulated. These are (1) attention to and understanding of the perspective of the various parties involved (2) the openness toward reformulating the original security problem considering these perspectives (3) experimentally-informed solution development and (4) the intent toward continuous improvement of the security solutions found. With this “lens” the question has been operationalised as to whether Design Thinking aspects are encountered in security practice.

The goal-oriented Design Thinking approach follows a different logic than the task-oriented policy and engineering approach that is common in the design of systems and systems’ security. Where the latter is organised top-down and work is done at each level on the basis of predetermined specifications, Design Thinking places primacy with end users and the approach is therefore organised bottom-up. Design Thinking also assumes leeway to discover and prioritise often unspoken questions and needs in the (broad) stakeholder field. The approach can therefore only be used in critical infrastructure security insofar as the cultural differences between the top-down and bottom-up organised processes can be bridged.

In the second part of this exploration, the developed lens is used to identify cases in which Design Thinking principles have been applied. This turns out to be effectively possible. 11 international cases and 11 cases from the Dutch critical infrastructure have been identified and are inspected in detail in this report. The analysis of the cases shows that Design Thinking approaches are possible in the infrastructure

practice. The first series of 11 international cases covers a large number of stakeholder categories. The second series of 11 covers various Dutch vital infrastructure sectors, especially the A category. Viewed from this perspective, Design Thinking is already being applied in the infrastructure practice.

In a further analysis, we also compare the forms in which Design Thinking aspects have been applied in the 22 cases. The order in which issues (leading to dissent) are identified and (partly unknown) solution directions are explored appears to vary. Also, solution styles vary between hierachical regulatory approaches, solutions left to markets and forms of network coordination. There is therefore not a single fixed "recipe" that is followed, but there is a need to give organisations the development space to include the methods in their processes. In all 22 cases, the underlying issues also turn out to be complex (wicked) hence unstructured. The use of Design Thinking is therefore evidently applicable, useful, of added value and complementary to engineering alternatives, which are more applicable when issues are more structured.

Where this report builds on examples with room for Design Thinking perspectives, the challenge for the future lies in the use of Design Thinking where it is not yet given space. Where the public sector is geared to implement classic so-called Type I innovations, the challenge lies with Type II innovations with more involved partners, developing problem definitions and with a need for openness to what works and what doesn't. The practical examples and identified cases througout this report are good practices of "Type II" innovations that are possible with Design Thinking.

To embed Design Thinking structurally, organisations will have to create the proper conditions. Room for Design Thinking implies that issues are not specified too prematurely, and that more dialogue and interaction is promoted with groups of actual stakeholders throughout the ideation and testing phase. This requires a very open attitude to questions and possible solutions and requires investment and administrative courage to overcome obstacles in organisational processes and regulations. In the vital sector space, the space for stakeholder orientation, experimentation and organisational learning will require active support from regional and national government.

In order to secure the national critical infrastructure in such a way that it remains resilient, the security problems identified in the first part of this study will have to be addressed as design challenges. Design Thinking can help to find focus and choose priorities. The recommendations that are part of this final conclusion are aimed at this development towards more people-oriented security. In order to build a resilient society, people must be able to recognise, interpret and adjust risky situations in a timely and adequate manner. OT security is best served by trained, properly informed people in every responsible position. Investing in Design Thinking can thus contribute to achieving organisational resilience in the vital sector.