European Journal of Operational Research 282 (2020) 627–643

Contents lists available at ScienceDirect

European Journal of Operational Research

journal homepage: www.elsevier.com/locate/ejor

Decision Support

Organizational vulnerability of digital threats: A first validation of an assessment method

Roland W. Scholz[a,b,c,*], Reiner Czichos[a], Peter Parycek[d], Thomas J. Lampoltshammer[d]

[a] Danube University Krems, Dr.-Karl-Dorrek-Strasse 30, 3500 Krems, Austria
[b] Institute for Advances Sustainability Studies (IASS), Berliner Strasse 130, 14467 Potsdam, Germany
[c] Department of Environmental System Sciences, ETH Zurich, ETH Zurich Universitaetstrasse 22, 8092 Zurich, Switzerland
[d] Department for E-Governance and Administration, Danube University Krems, Dr.-Karl-Dorrek-Strasse 30, 3500 Krems, Austria

ARTICLE INFO

Article history:
Received 2 January 2019
Accepted 12 September 2019
Available online 20 September 2019

Keywords:
Problem structuring
Decision analysis: Vulnerability assessment
Resilience management
Digital transformation

ABSTRACT

We present a Strengths, Vulnerability, and Intervention Assessment related to Digital Threats (SVIDT) method, which provides a problem structuring and decision support for organizational vulnerability and resilience management with respect to changes of the digital transition. The method starts from (i) a multi-level actor analysis, (ii) identifies strengths and weaknesses of organizations, (iii) constructs digital threat scenarios and provides judgment-based expert assessments on the organization's vulnerability, (iv) develops intervention scenarios for tangible threat scenarios, and (v) suggests win-win action scenarios when referring to the multi actor system analysis as for strategic management. A first validation and application includes a structural analysis of the response patterns and a quantitative and qualitative appraisal of the organizations' managers. This validation is based on an application of the method to 18 German and Austrian organizations of different types and magnitude. We show how the basic concepts of vulnerability (i.e., sensitivity, exposure adaptive capacity) can be quantitatively operationalized when constructing consistent combinations of threat and intervention scenarios. The validation approaches indicate that the method provides meaningful data and assessments and that the managers provided a positive feedback on the method and the recommendations which they received. It is further deliberated whether the assessment method supports organizations' specified resilience management in an overly complex, systemic digital transition in a (semi) quantitative manner. In addition, we discuss needs for future research regarding practical utility of SVIDT, as well as the positioning of SVIDT in relation to soft operational methods and other methods of operational research.

1. Introduction: Organizational vulnerabilities and the SVIDT method

1.1. Purpose and goals of the paper

The digital transformation is one example of systemic change which provides fundamental risks with "significant tangible" and "perplexing uncertainties" (Rosenhead, 2006) to all of domains society. The purpose of this paper is to provide a comprehensive operationalization, application and validation of the Strengths, Vulnerability, and Intervention Analysis related to Digital Threats (SVIDT) method (Scholz, 2017a) to *organizations*. SVIDT may be conceived as a Problem Structuring Method (Ackermann, 2012; Eden & Ackermann, 2006; Mingers & Rosenhead, 2004) and soft operational decision analysis method (Checkland & Scholes, 1990) (Mingers, 2000). SVIDT starts from (i) a multi-level actor analysis, (ii) identifies strengths and weaknesses of organizations, (iii) constructs digital threat scenarios and provides judgment-based expert assessments on the organization's vulnerability, (iv) develops intervention scenarios for tangible threat scenarios, and (v) suggests win-win action scenarios when referring to the multi actor system analysis as for strategic management (Friend & Hickling, 2005). The application is been done in a collaborative, transdisciplinary manner, in which the (experiential) subject knowledge of practice experts is linked with the methodological knowledge of operations research (OR) consultants and rigor and in-depth knowledge about the digital transformation scientists

* Corresponding author at: Department of Environmental System Sciences, ETH Zurich, ETH Zurich Universitaetstrasse 22, 8092 Zurich, Switzerland.
E-mail addresses: roland.scholz@emeritus.ethz.ch, roland.scholz@donau-uni.ac.at (R.W. Scholz).

https://doi.org/10.1016/j.ejor.2019.09.020
0377-2217/

from OR and information technology researchers. We argue that transdisciplinarity, i.e., the collaboration among organizational managers and or practitioners and scientists may be needed to overcome some deficits and constraints of OR practice, as they have been described by Rosenhead (2006) in complex settings such as managing the digital transition of companies. Some scientists argue that the substitution of labor-related cognitive operations by computers are inducing more changes in production, trade, and markets than the first Industrial Revolution (Brynjolfsson & McAfee, 2012; Helbing, 2015; McAfee & Brynjolfsson, 2017; Porter & Heppelmann, 2014).

The SVIDT method extends the concept of risk to the vulnerability concept (Scholz, Blumer, & Brand, 2012). This is shown in the following sections of the introduction as well as that the SVIDT method emerged – besides from OR – from *decision research* and *transdisciplinarity*.

1.2. From risk to vulnerability in digital transformation management

From a decision theoretic (Keeney & Raiffa, 1976) and entrepreneurial management (Hisrich & Ramadani, 2017) perspective, a company's or organization's adaptations and interventions are traditionally managed by means of *risk analysis*. In general, companies and organizations evaluate business strategies in light of changes in key performance indicators, e.g., turnover, market share, cash value, etc. for commercial organizations and number of members, publicity, etc. for non-commercial organizations. Digital-technological innovations, for instance, may be viewed as *threats* as they can have negative impacts, which in turn may affect the viability of organizations and call for fundamental *adaptive action*. Markets for certain products (e.g., mechanical typewriters or printed matter for surface mailing) or intra- and interorganizational processes (e.g., personal operation-based calendars or logistics management) might be eliminated and new types of actions needed. Both internal and external communications are undergoing fundamental changes, and if organizations fail to adapt in a timely manner time, then digital innovations become threats.

Consequently, digitalization can be viewed as an *environmental risk*. In general terms, *risk* can be conceived as an *evaluation function of the loss potential* in a certain situation, with uncertain outcomes. If the losses only are considered, we speak about *pure risk;* if the positive outcomes are integrated, we talk about *speculative risk* (Brachinger & Weber, 1997; Scholz et al., 2012). Historically, there are two major approaches for defining risk, a *decision-* or *choice-based* approach and an *exposure-based* approach. The *decision theoretic approach* starts from the idea that humans (or human systems as companies, societies, etc.) make decisions. The *exposure-related approach* emerged from the fields of toxicology and insurance (Paustenbach, 2002). Here, the *voluntariness* – and thus the freedom to make a decision – is not postulated. The exposure-related conception becomes a decision theoretic of the risk is perceived and a reduction or elimination of exposure is theoretically thinkable by the exposed agent (e.g., a company gives up business).

In a decision theoretic approach, a decision-maker has a *choice* between at least two different alternatives (in a general risk situation, between a set of alternatives $A_i \in A$; the nomenclature for all variables may be found in supplementary information SI1). In a *pure risk situation*, with the choice of an alternative A_i, a discrete number of *negative-valued events* ($E_{i,j} \in \mathfrak{E} = E$) may result with certain *probability* ($p_{i,j}$). If we denote the probability distribution as P, risk is a function of the space of decision alternatives A, the space of probability distributions P, and the set (valued) possible events E, formally:

$$(1)\quad r = f(A, P, E)$$

In *speculative risk*, a decision-maker also acknowledges the utilities of all positively or negatively valued events from a risk or loss perspective. We can learn from *prospect theory* (Kahneman & Tversky, 1979) that what is considered a loss and thus the size of a risk may change according to the view taken. Thus, the perspective taken has to be defined when constructing a risk function.

In the exposure-oriented approach, risk is a function of *exposure* and *sensitivity*. Usually, exposure is operationalized by probabilities, and the sensitivities are the impacts of specific negative outcomes of a certain E, which may result when a particular event takes place. In semiformal terms, this may be expressed by:

$$(2)\quad r' = g(exposure,\ sensitivity) = r'(P, E)$$

The SVIDT method goes *beyond risk management*. This is due to the incorporation of the *adaptive capacity*, *AC*. Please note that risk considers threats, i.e., potential negative events, from an *a priori event perspective*. Thus, the above-described risk function (2) includes events that may appear with certain probabilities, but that have not yet appeared. The adaptive capacity changes this perspective and describes the effects of the potential actions a decision-maker may take if a specific event with negative outcomes has actually taken place. One may think about a retail company (e.g., a bicycle retailer) around the year 2005 who missed the shift from phone and surface mail-order systems to (partly automated and available 24/7) electronic-order systems. In this case, the company could have faced continuing losses of market share over a number of years. The adaptive capacity represents the potential of the bike company to compensate for the possible loss of market share by implementing missed as well as perhaps additional new digital technologies at a later stage. Actions taken after a certain threat has become real are called *interventions*. In the context of new digital technologies, interventions are most closely linked to innovations. Often, sufficient financial and personal resources may be considered the main components of *adaptive capacity*. Referring to the above notion of risk as $r = r' = g(P, E)$, we define *vulnerability* as a function that comprises the *a priori* risk evaluation and the assessment of the *a posteriori* (i.e., after event) adaptive capacity of a decision-maker to reduce losses that (may) have occurred as the impact of negative events.

This may be expressed as

$$(3)\quad vul = h(P,E,AC) = vul(P,E,AC)$$

where $AC = (AC_{m,j}) = (I_m(T_j))$, $m \in \mathfrak{M}$, denotes the bundles of actions or *interventions* (I) that may be taken to maintain the *viability* of an organization posterior to a negative event, i.e., a threat scenario T_j that has been assumed to have taken place. If quantified, *specified resilience* is sometimes defined as $1 - vul$ (Scholz et al., 2012).

In the context of the operationalization of SVIDT the adaptive capacity is of special importance. Due to the impossibility to quantify probability distributions for a large set of digital innovations in artificial intelligence, internet of things, cloud computing, speech processing, pattern recognition, etc., the presented operationalization of SVIDT identifies a set of consistent, incongruent (dissimilar) high threat scenarios. When assessing (apriori) exposure and sensitivity and exposure and (posteriori) the adaptive capacity, i.e., the keeping of the viability by counteracting by well-constructed and (semi-quantitatively) assessed intervention strategies.

1.3. Theoretical roots of SVIDT

As mentioned above (see also Scholz, 2017a) besides OR, the SVIDT approach is rooted in *decision research, risk analysis,* and *transdisciplinary transition and resilience management*. Vulnerability is the complement to resilience, which has become a key concept

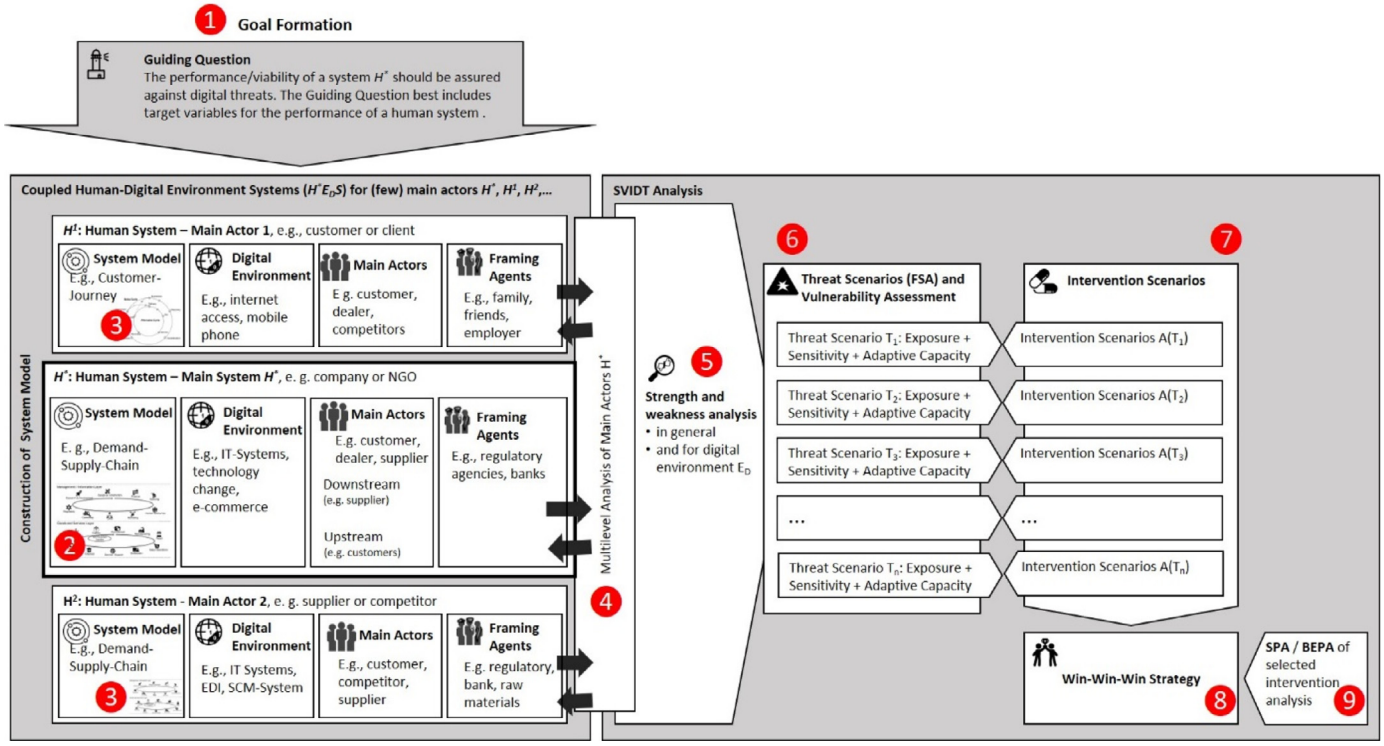

Fig. 1. The nine steps of the SVIDT method (figure taken from Scholz, 2017a).

in sustainable transitioning (Adger, 2000, 2006). The presented operationalization of SVIDT can be viewed as an expert judgment-based quantitative approach of the upcoming resilience research. Transdisciplinarity, conceived as integrating knowledge from science and from practice, is key, as SVIDT may be seen as a research method that goes beyond consultancy-based risk assessment. Mutual learning among science and practice is an essential element of applying SVIDT methodology. Thus, we may distinguish between the managerial experts from a specific organization and the (practical) operation research consultant and the method and (for instance digitalization) subject-oriented scientists who collaborate in complex cases (for helping in coping with complexity) or in the course of adapting and developing the method. Transdisciplinarity has many similarities with some of the many variants of action research such as community based-participatory action research (Wallerstein & Duran, 2010). Yet transdisciplinarity conceives scientists serving the public good and does not for the researcher's actionist's bias of interest as it is common for action research (Eden & Smithin, 1979; Scholz, 2017c). Another difference is that science practice interactions are expected to develop research (Scholz, Lang, Wiek, Walter, & Stauffacher, 2006) which has become a characteristic of research oriented action research (Eden & Huxham, 2006, p. 399).

SVIDT is a hybrid method. It starts from a *multilevel system model* (see Fig. 1, Step 2 and Step 3). The multilevel analysis is performed with the help of the hierarchy postulate of the Human Environment System (HES) framework (Scholz, 2011). This provides a template for conceptualizing drivers and rationales for individuals, organizations (i.e., commercial and NGOs), or framing agents such as ministries (institutions), politicians, or courts (Scholz, 2011), and other main actors (see Step 4). The construction of an impact matrix-based system model (including the construction of consistent scenarios via Formative Scenario Analysis (FSA); Missler-Behr, 1993; Scholz & Tietje, 2002) for constructing threat scenarios (see Step 6) and corresponding intervention scenarios (see Step 7) is the core of SVIDT. A thorough understanding of the strengths and weaknesses (Step 5) of an organization has to precede these steps. This phase can be supported by applying, e.g., a SWOT analysis. A detailed, condensed list of *digital threats and changes* (dTCs) has to be built as a basis for constructing intervention scenarios. A multicriteria decision assessment is involved by considering a set of weighted key-performance parameters in order to assess the sensitivity and adaptive capacity. Step 8 refers to creating synergies among the key agents, which have been identified in Step 4. The final step (Step 9) includes a qualitative system analysis referring to Sustainable Potential Analysis (SPA) (Lang, Scholz, Binder, Wiek, & Stäubli, 2007) and Bioecological Potential Analysis (BEPA) (Scholz & Tietje, 2002). Both approaches provide qualitative criteria and heuristics (e.g., the change rate of a system should not exceed critical boundaries) in regard to the evaluation of key facets of viable and sustainable systems. Together with the quantitative vulnerability scores, they build the foundation for selecting intervention strategies for an organization facing dTCs.

1.4. Specifics of digital threats and changes (dTCs)

The digital transition is characterized by a strong, concise trajectory toward the digitalization of all domains of life. Yet, there is extraordinary (perplexing) uncertainty regarding the timing and success of digital technologies. This can be seen in the failed predictions made by significant pioneers of artificial intelligence (AI), e.g., Herbert Simon's 1965 statement: "Machines will be capable, within twenty years, of doing any work a man can do" (see Velik, 2010) or Marvin Minsky's 1970 vision: "In from three to eight years we will have a machine with the general intelligence of an average human being" (see Velik, 2010). On the other hand, there have been precise predictions, such as Moore's Law on technological progress (Courtland, 2015), which led to an unexpected decline in the volume and price of storage capacities. Automated driving systems may be considered another example. For how many years might a London cabdriver expect to be able to pursue the work that feeds his family?

Theoretically, it may be of interest that the two major components involved in vulnerability, i.e., risk and adaptive capacity, show some *strategic complementarity*. *Investing in lowering risk* means to invest in lowering exposure (i.e., the probability of being affected by a negative event) and in lowering sensitivity (i.e., reducing the damage from a negative event by being more robust). From a pure risk perspective, this means to strongly invest in new digital innovations and to become a digital-technology forerunner. We may note that risk prevention is related to known future negative actions. *Investing in adaptive capacity* means preparing an organization to cope with negative effects if an uncertain negative event has taken place, and then repairing the negative impacts and adjusting to maintain viability. *Focusing on lowering the risk* is *risk aversive,* but it means promoting innovation. Focusing on adaptive capacity means to prepare for action by increasing financial, human, knowledge, and other capitals. Focusing on adaptive capacity is risk seeking. Thus, whether to invest more in order to reduce risk or to increase adaptive capacity is a *normative decision,* and the weighting between the two is called normative value. The concept of normative value can be extended further, by not only addressing the weighting between risk reduction and increase of adaptive capacity, but also by introducing additional parameters, such as a normative representation of the formal mission or creed of the organization (e.g., "we live sustainability") and the effect of a particular dTC scenario on this normative value.

Multiple transformations at all levels and domains of society are challenging and may be denoted as *systemic risks*. Systemic risk is related to uncertain and unknown dynamics in complex, highly interconnected systems, and it is linked to "uncertainty about one's uncertainty," i.e., uncertainty about the probabilities or density functions of future events. This second-order uncertainty has been called *ambiguity* (Einhorn & Hogarth, 1986; Hogarth & Kunreuther, 1985), for instance, in regard to when a particular dTC may become relevant for an organization. This also includes systemic risks, which emerge in complex, highly interconnected systems; the term *unintended side effect* (Scholz et al., 2018; Sugiyama et al., 2017) represents this feature. Resilience research distinguishes between *specified resilience* and *general resilience*. We talk about specified resilience when the (uncertain future) events are known. Specified resilience is the complementary concept of vulnerability. A system that has general resilience has the capacity to cope with the unknown. In principle, we hope that *general resilience* will emerge if vulnerability to a wide range of different dTCs is reduced.

The latter leads us to another challenge. As uncertainty is ubiquitous, a vulnerability assessment would require the construction of possible events and related probability distributions at all stages of analysis (see Fig. 1). Given the complexity and fundamental uncertainties related to (highly interdependent) events and dTCs, this is too challenging. In the present application of SVIDT, we delimit uncertainty assessment to judgments of certain salient scenarios of dTCs. In line with reducing complexity, we will also focus on the notion of *pure risk* and only model (and quantify) the losses caused by the former-mentioned scenarios.

Part 2 of this paper comprises the detailed description of the SVIDT methodology. In particular, we present the operationalization of the vulnerability score, based on a multilevel analysis of the actors and the construction of well-selected threat scenarios and corresponding intervention scenarios. Part 3 includes two types of validation of the SVIDT method, i.e. a structural analysis of the vulnerability scores and an appraisal of the management of the involved companies. This is followed by a thorough discussion of results in part 4, including needs for future research regarding practical utility, as well as the positioning of SVIDT in relation to soft operational methods and common methods of operational research. Part 5 then closes the paper with the authors' conclusion.

2. Description of the SVIDT methodology

2.1. Understanding the organization

Step 1 (all steps refer to Fig. 1), Goal Formation, is the most important one. Given the experience of more than 40 transition studies (Scholz & Steiner, 2015), a well-formulated, concise *Guiding Question,* the exact wording of which must be discussed with the key members of the organization, is crucial for applying SVIDT. The *Guiding Question* includes the description of what parts of the organization become subjects of the application (e.g., organizational system boundaries, prospective time range for intervention) and of what are the objectives and outcomes of the SVIDT application (e.g., how to include the members of the organization). The *Guiding Question* should serve as a pervasive reference throughout all steps of applying the SVIDT method.

The objective of Steps 1–4 is to produce a qualitative and visual multisystem model. The key processes and key actors with respect to the digital changes should be included. The practical work starts with a description of a system model of the organization. This description has to include a comprehensive inventory of basic organizational data (foundation, legal form, number of employees, turnover, etc.), the product portfolio, and an organizational chart. For embedding an organization, a supply–demand chain model is usually meaningful. The model should include all downstream inputs by material and information, a rough model of inner-organizational activities, and upstream customer relationships. For (traditional) companies, the Business Model Canvas (Osterwalder & Pigneur, 2010) is often a suitable tool for describing the inner processes. If we consider ICT companies, a model may include specific major transitions, e.g., the impacts of cloud computing (Weinhardt et al., 2009) or market changes due to the introduction of blockchain technology (Ivanschitz et al., 2018).

Given the fundamental changes of the digital transformation, framing agents play a specific role. By framing agents, we understand not only governmental actors but also global ICT companies' key players or leaders in industrial associations. To get a better access to the rationales and drivers, we distinguish between individuals, small groups, and other forms of groups; organizations (commercial and non-commercial); institutions (i.e., governmental or supranational organizations); societies (in particular, political and cultural/religious leaders); and supranational systems (such as the EU). This refers to the *hierarchy postulate* of the Human–Environment System (HES) framework, which describes drivers and rationales (see Chapter 15 of Scholz, 2011) of the identified key actors when referring to primary disciplines of these systems (e.g., psychology for individuals, business science for companies, or administration sciences for institutions) and thus goes beyond, for instance, the consideration of one-level networks.

2.2. Constructing an impact-variable-based simple model of the organization

The SVIDT system analysis (Step 4) comprises two main blocks. First, we provide a qualitative description of the processes, key actors (and their functions and levels according to the hierarchy level of the HES framework), and framing conditions. Second, we construct a (relatively) small but – with respect to a *Guiding Question* – sufficient set of variables or *impact factors* (called $d_{\hat{m}}$). These impact factors should represent all system variables which represent dTCs (such as big data, artificial intelligence, voice processing) related to the digital transformation. The impact factors should describe the current state and the changes of the organization in light of the *Guiding Question*. This is a common procedure in the formation of scenarios. For modeling the changes, for each impact factor, different levels – i.e., different values or specifications $d_{\hat{m},n_{\hat{m}}}$ –

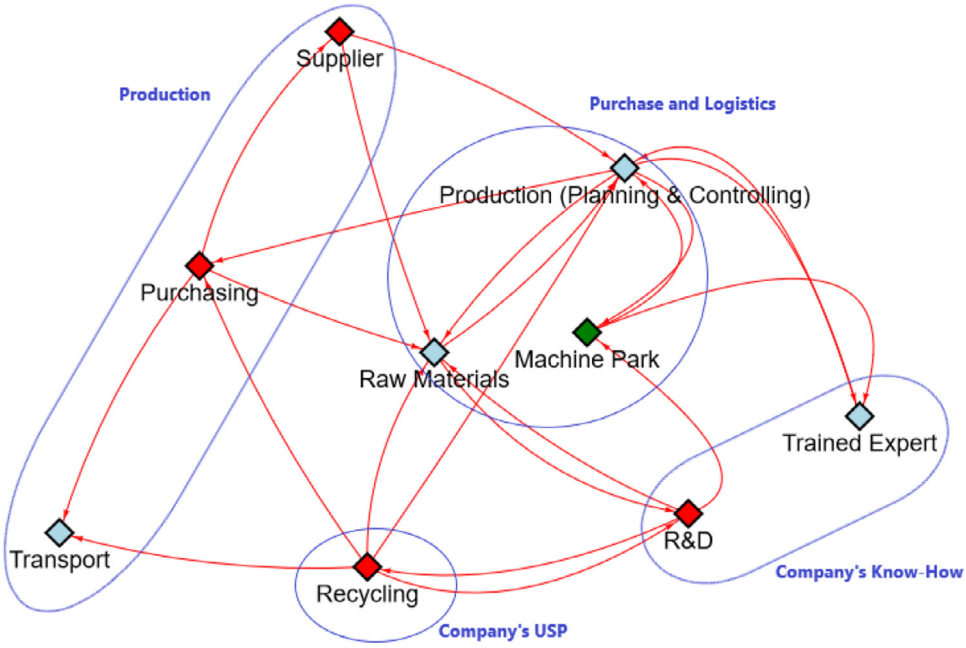

Fig. 2. System graph and (suggested) subsystems for a mattress producer (red arrows represent strong impacts; red diamonds have a higher active sum than passive sum; blue diamonds are the opposite; green diamonds have a balanced affection ratio).

that an impact factor may take have to be formulated. For the simplest form, $n_{\hat{m}} = 1$ considers the case in which nothing changes compared to the status quo, and the variable $d_{\hat{m},n_{\hat{m}}}$ for $n_{\hat{m}} = 2$ means that a specified change has taken place. The impact factors $D = \{d_1, \ldots, d_{\hat{m}}, \ldots, d_{\hat{m}_D}\}$ are also called *descriptors*, as they serve to describe the status quo and the changes of a system in (semi)quantitative terms.

After having defined the impact factors, the relationships or impacts among these factors are assessed. This is done in order to gain insight into the system and its subsystems. Given the incomplete knowledge, quantitative relationships in the form of mathematical functions (which would allow for system dynamics) can be defined only among a very small number of factors – if at all. Thus, in the context of applying SVIDT to organizations, the *causal impacts* between two impact variables $d_{\hat{m}_i}$ and $d_{\hat{m}_j}$ are assessed on an ordinal scale (e.g., no impact, moderate impact, and large impact). These ratings are called *cross-impact scores* and represented as $ci_{\hat{m}_i,\hat{m}_j}$. Please note that only the strengths of direct impacts have to be assessed or judged. This calls for considering all indirect relationships when making the judgments, and judgments have to be altered if some impact factors are skipped or changed. For practical purposes, this means that the judgment has to be provided twice as the other relationships are unknown when the first relationship is assessed (see Scholz & Tietje, 2002). Usually, the ratings of causal relationships have to be discussed, adjusted and – in the event of disagreements – reach consensus among the study team members.

Fig. 2 presents a graphical representation of the cross-impact ratings of a mattress company. Based on the relationships among the impact strengths and logical reasons, the system graph allows for the formation of system variables. The cross-impact matrix $CI = (ci_{\hat{m}_i,\hat{m}_j})$ allows further insight into the research team's view of the organization. We can gain insight into how much a variable affects all other variables by summing up the impact strengths a variable has on all other variables. This is called *active sum* and reads formally as:

$$(4)\quad ci_{m_{i,\cdot}} = \sum_{j=1}^{\hat{m}_D} ci_{\hat{m}_i,\hat{m}_j}$$

Likewise, we can gain insight into how much a variable is affected by the other system variables when summing up the impacts a variable receives from others. This is called the *passive sum:*

$$(5)\quad ci_{\cdot,m_j} = \sum_{i=1}^{\hat{m}_D} ci_{\hat{m}_i,\hat{m}_j}$$

There are other options such as studying loops of three and larger order or assessing to what degree a variable is integrated.

2.3. Identifying potential digital threats

In order to prepare a modeling of relevant dTC *scenarios* to which an organization may be exposed, a qualitative identification of the weaknesses of the organization is helpful. This can be accomplished by performing a *strengths–weaknesses analysis* (Step 5). The team may develop a list of perceived general and digital technology-related weaknesses and strengths. In addition, a SWOT analysis (Dyson, 2004; Helms & Nixon, 2010) or identification of the types of innovations considered or suggested by internal and/or external actors in the past can be applied.

In reviewing the work of 18 project groups for the first application of SVIDT reported below, a total of 46 different changes were identified (Sczesny, 2018). These include general changes such as big data, cloud computing, or digitalized customer and production processes, market changes as indicated by the concept of the prosumer, or more elementary processes such as digitalized payment. The list of dTCs that results depends on the (set of) the organization, the ongoing transitions in the ICT business, and the knowledge/competence of the team. These aspects will not be considered in depth in this paper.

2.4. The constructions of digital threats and change scenarios

A key concept of the SVIDT method is to construct a small set of *consistent, essentially different dTC scenarios,* T_j (see Fig. 3, upper-left boxes A–C; in this case, given the number of threats and their contingencies, one to three dTC scenario(s) has/have been selected for each subsystem). For each selected threat scenario, *consistent* intervention scenarios, $I_{m,j} = I_m(T_j)$, will be constructed.

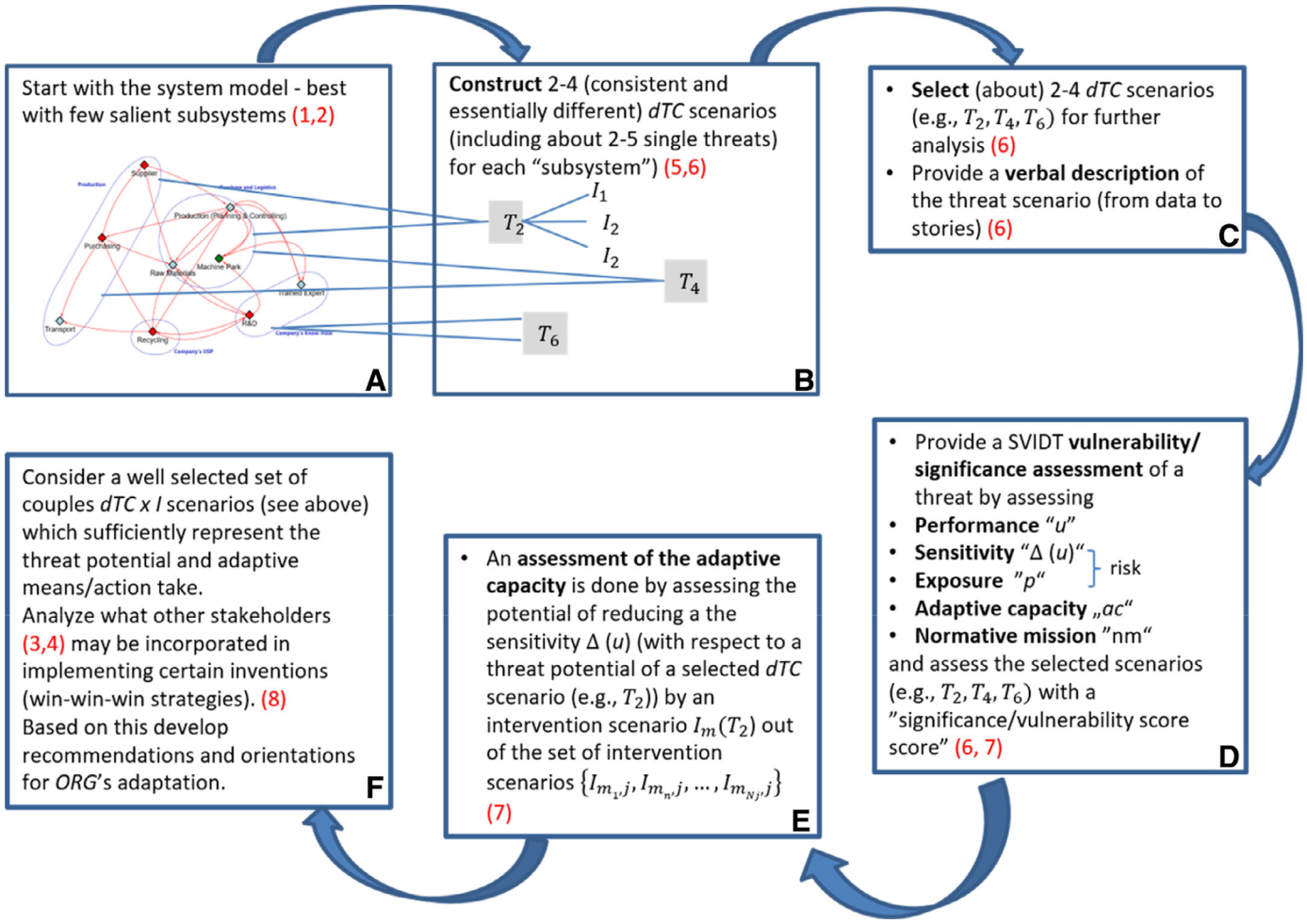

Fig. 3. From system representation *A* via (general or subsystem-related) dTC scenarios, *B* and *C*, a quantitative assessment of vulnerabilities *D*, and adaptive capacity assessment *E* to win-win-win strategies for organizations, *F*.

In general terms, a *scenario* is a complete combination of levels of impact factors (Scholz & Tietje, 2002, p. 105). Thus, a dTC scenario, T_j, $j \in \mathfrak{J}$, is a vector whose impact factors are levels of single dTCs, $t_{j_n,j}$, $n \in \mathfrak{N}$:

$$(6)\quad T_j = (t_{j_1,j},\ldots, t_{j_n,j}, \ldots, t_{j_N,j})$$

The double-index j_n describes what level the n-th impact factor (i.e., threat) takes for the dTC scenario T_j. The set of all dTC scenarios is labeled $T = (T_j)$.

When constructing dTC scenarios, we refer to the standard procedure of impact-factor-based scenario construction (see Götze, 1990; Missler-Behr, 1993; Reibnitz, 1992; Scholz & Tietje, 2002). In its simplest and often (pragmatically) applied form, each single dTC $t_{j_n,j}$ appears on only two levels. Usually, $j_n = 0$ represents the threat not occurring, and $j_n = 1$ will be interpreted as a digital change occurring. Assuming 10 potential dTCs with 2 levels, there are 1024 dTC scenarios. As it is impossible to assign a reasoned probability function to these scenarios, the consistency of dTC scenarios plays an important role. The strategy taken is the following: First, a *consistency analysis* excludes inconsistent dTC scenarios. This is done by judgments on the (logical consistency and practical feasibility) on all $(J * (J-1)/2)$ pairwise combinations of the N dTCs. Then, a small set of *essentially different* (*complementary* consistent dTC scenarios are selected from the set of consistent dTC scenarios which are supposed to sufficiently represent the space of future digital environments. Here, in general, essentially different means that the selected dTC scenarios do not only differ by one or two levels of impact factors (i.e., threats) but build kernels of clusters of clusters of scenarios of a certain type. An algorithm can be used to extract essentially different dTC scenarios (Tietje, 2005). This is the subject of Step C in Fig. 3.

After the assessment vulnerability (see D), in Step E, (consistent) intervention scenarios, $I_{m,j}$, for each dTC scenario, T_j, that remains after the selection process are constructed:

$$(1)\quad I_{m,j} = I_m(T_j) = (I_{m_1,j}, \ldots, I_{m_n,j}, \ldots, I_{m_{N_j},j})$$

Theoretically, one may think about constructing a probability distribution among the consistent or among the finally selected dTC scenarios. We argue that, in general, this is beyond the limits of knowing. Instead, learning should take place based on investigating and assessing the impacts that the small set of complementarity dTC scenarios may have on key performance indicators. A critical issue is that we have to distinguish between *theoretical intervention* scenarios and *realistic interventions*. The latter refers only to what is within the range of the company's current action potential. The analysis of both types of scenarios may be of interest. When comparing the *theoretical* and the *realistic*, consultancy strategies can be developed.

2.5. Quantifying vulnerability

In order to assess the impacts of the dTC scenarios, we construct a quantitative vulnerability score, $vul(T_j)$, for an organization. The score is the outcome of a kind of *stress test*. Simplified,

this vulnerability score can be considered a function of the threats and the organization's adaptive capacity to cope with them, i.e.:

(7) $vul(T_j) = vul(P,E,AC) = vul(r(T_j), ac(T_j))$

The stress test is a thought experiment and assesses how the key performance of an organization is affected by the digitalization of internal processes, relationships with customers or members, the types of products required (i.e., demand function), changing legal requirements, etc. (see Fig. 1). The adaptive capacity also includes an assessment of how *win–win situations* (see Fig. 1, Step 9) can be created by new types of collaboration with other partners of the supply–demand chain.

Actually, the relationship between (prior) risk assessment and (post-)adaptive capacity appraisal has to be specified and modeled, and it depends on time and the (stand-by) time range for sensitivity assessment. Practically and in the application below, first a *risk score* $r(T_j)$ can be assessed for the assumption that an organization continues its present mode of operation without any adaptation(s) to digital innovation for a certain *time period*, e.g., three years. Then, the impacts of a dTC T_j on the different *key performance indicators* (KPIs) are assessed. This is an assessment of the *sensitivity* of the organization. By providing expert judgment on the likelihood that the dTC T_j will become real in the time period considered, a risk score can be calculated. Then, we consider the selected intervention scenarios, $I_{m,j}$, and evaluate how much the assessed loss of the different KPIs can be reduced. This is a quantitative assessment of the adaptive capacity given salient dTCs T_j and corresponding intervention scenarios $I_{m,j}$. Finally, in the present application, the vulnerability score is simply a weighted sum of risk and adaptive capacity:

(8) $vul(T_j) = vul(r(T_j), ac(T_j)) = \hat{w} * r(T_j) - (1-\hat{w})ac(T_j)$ with $0 \le \hat{w} \le 1$

Here, the weight $\hat{w}$ reflects the organization's (business) strategy to avoid any risk and potential losses. If we consider the vulnerability score as an (early) warning indicator, a high $\hat{w}$ has to be taken in the case of a *risk-averse organization* that wants to avoid any potential loss. By contrast, an organization may take a conservative strategy and not want to be the first mover with respect to digitalization. If an organization's only interest is to strengthen its ability if certain changes in the practices of other organizations have taken place, then $\hat{w}$ should be low. Thus, we denote $\hat{w}$ ($\sum_{n=1}^{n=m} \hat{w}_n \le 1$) as a normative business-strategy parameter. Additional normative parameters (see Section 1.5; see Step D in Fig. 3) can be introduced, if necessary.

Theoretically, probability distributions can be constructed for (consistent and essentially different) dTC scenarios that are assessed. Moreover, the probability that an intervention scenario provides a certain reduction of an estimated loss (or a probability distribution on the reduction of losses) could be introduced to integrate vulnerabilities resulting from different dTC scenarios. Methods for doing this have been provided by Gottschalk, Scholz, & Nowack (2009), Scholz & Hansmann (2007), and others. However, such a quantification goes beyond the available knowledge if we want to provide an estimate of estimates of probability distributions for all possible future dTC scenarios. This would require that the space of all future dTCs is known and can be constructed. Thus, a composite vulnerability score $vul(T)$ based on equal weighting or other algorithms (e.g., worst case) on a small (sufficient) set of well-selected, different dTCs representing the space of digital technologies to which a company has to adapt is more meaningful (if T denotes a set of selected scenarios; this is discussed in the last two sections of 5.2). We now briefly sketch how different assessments can be operationalized.

2.5.1. Defining the "total performance" of an organization

When defining total performance, we refer to a common multicriteria utility assessment. The team and the representatives of the organization have to define the main criteria of the current performance and to assess – on a [0.1] scale – what *degree of performance fulfillment* compared to the ideal level of performance 1 the organization is currently providing. This results in a utility vector $u = (u_1, \ldots, u_i, \ldots, u_I)$. In a second step, weights $w = (w_1, \ldots, w_l, \ldots, w_I)$ of the performance scores, associated with each KPI respectively, with $\sum_{l=1}^{I} w_l = 1$ have to be assessed. This provides the *total performance score*

(9) $u_{tot} = \sum_{i=1}^{I} u_i w_i$

Practically, the different utility criteria for a well-known set of KPIs are known by the management board of a company or organization. The degree of performance fulfillment can be assessed based on subjective expert judgments or – for some variables – by quantitative assessment. For instance, rate of turnover, number of new members of an NGO, or customers, etc. can be well accessed in a quantitative manner. Of course, other models for constructing performance and utility scores may likewise be used (Saaty & Ergu, 2015).

2.5.2. Assessing risk

The *potential loss* of *total performance* u_{tot} caused by a dTC scenario T_j represents the *sensitivity* (see Formula 2). We may define this loss simply as the weighted sum of losses by T_j over all KPIs (i.e., utility attributes) compared to the utility at the present time, denoted as T_0:

(10) $\Delta(u_{T_j}) = \Delta(u(T_j)) = \sum_{i=1}^{I} w_i(u_i(T_0) - u_i(T_j))$, for all selected T_j, $j \in \mathfrak{J}$

The loss (potential), therefore, is simply the difference Δ between the utility at the present time and that caused by T_j after a certain time period when not adapting to digitalization.

For assessing the likelihood p_{T_j} that a scenario becomes real, there is no choice other than relying on expert judgments. Thus, the risk score is:

(11) $r_{T_j} = r(T_j) = p_j * \Delta(u_{T_j}) = p_j * \sum_{i=1}^{I} w_i(u_i(T_0) - u_i(T_j))$, for all selected T_j, $j \in \mathfrak{J}$

Expert judgments should be based on (a) general scientific literature on the speed of digital-technology innovation (see, for instance, Bojanova, 2014; McAfee & Brynjolfsson, 2017) and (b) on the experience of experts of different part of the organization. We described above (see also Fig. 3) that we are selecting a small set of essentially different dTC scenarios. The idea is that we assess the risk for all these scenarios. We may then take, for instance, the maximum or mean value as the *risk score*.

2.5.3. Assessing adaptive capacity

Given a dTC T_j and the estimated loss $\Delta(u_{T_j})$, the challenge is to assess how much a bundle of interventions, i.e., an intervention scenario $I_{m,j} = I_m(T_j)$, might reduce the loss (after a certain time period). For assessing adaptive capacity, there are two options. One refers to *theoretical* and the other to *realistic* intervention scenarios. Commonly, whether a scenario is realistic depends on whether the organization has the capability to implement the means. Here, financial and human resources (in particular, digital-technology knowledge) are main factors. For a consultancy strategy, a (backward-planning type) option would be suitable. When constructing an ideal intervention strategy $I^*_{m,j}$, a company can learn what means have to be acquired in order to avoid vulnerability. In a realistic-based vulnerability score, the company may learn about the limited or given options to adapt with the given means.

The adaptive capacity *ac* for an intervention scenario $I_{m,j}$ is:

(12) $ac(I_{m,j}) = acs(I_{m,j}) * \Delta(u_{T_j})$ with $m \in \mathfrak{M}$, $j \in \mathfrak{J}$

Here, $acs(I_{m,j})$ may simply be an expert assessment of what percentage of the total performance loss can be compensated for by a well-selected (realistic or ideal) intervention strategy.

2.5.4. Assessment of the vulnerability score

For assessing the vulnerability score, it is necessary to weigh how much effort is spent on *(a priori)* proactive steps taken to avoid risk in relation to the *(a posteriori)* adaptive capacity to adopt digitalization means at a later point of development. This can be accomplished by a risk-avoidance vs. adaptation-building weighting or score $\hat{w}$. Thus, Formula 3 provides a vulnerability score.

2.6. "Gentle validation" of the SVIDT method

When presenting a first validation of SVIDT, we follow two lines. First, we provide a *distributional structure analysis.* In a second line, we report the judgments of study teams and of managers of organizations who participated in a first application of the method. This is conducted in a quantitative as well as qualitative manner. We call this procedure "gentle validation" (Scholz, 2018), as there are no hard data that show, for instance, whether the risk and vulnerability are valid in the sense that a higher score would be linked to actual losses of KPIs.

2.6.1. Distributional structure analysis

Distributional structure analysis includes an appraisal of whether the distributions of the key parameters (e.g., risk, adaptive capacity, normative value, and vulnerability, total performance, sensitivity (reduction of performance) provide distributions of data that appear reasonable from a distributional perspective. The idea of structure validation (whose ideas are related linguistic structure analysis, Harris, 1954) has epistemological and psychological roots. If we study (performance) indicators in regard to nature, human systems, or technology, we learn that performance indicators in complex systems are somewhere between normally and log-normally distributed. This has been conveyed by the phrasing "life is lognormal" (Limpert, Stahel, & Abbt, 2001); most data in environmental systems are log-normally distributed. Thus, if distributions should result whose forms cannot be well justified, this may be seen as evidence that the SVIDT method can be refuted. We may consider the applied method as a kind of extended outlier analysis that is searching for anomalies or discordant data to a reference. Specific data (in this case, a certain method) are sorted out if data are provided that do fit not meaningfully into a frame of interpretation.

2.6.2. Construct validation by comparing subgroups

In principle, construct validation is an umbrella concept of validation (Cronbach & Meehl, 1955). It "refers to the extent to which an instrument or method [here, the SVIDT method] measures the theoretical entity ('the construct') that it was designed to measure" (Scholz & Tietje, 2002, p. 336). A common means of construct validation is that hypotheses about differences under experimental conditions are formulated, e.g., on how two groups with different exposures/features differ. We did not include such an experimental procedure. Yet, we may compare, *a posteriori,* different types and organizations and may learn about the method's descriptive potential by comparing the differences. If the differences are plausible, this can be seen as a (soft) argument that the method shows some validity and vice versa.

2.6.3. Appraisal SVIDT application by the managers of the organization

A common procedure used to validate a diagnostic or therapeutic instrument is to ask those who have been subjects of the application whether it is meaningful, useful, and beneficial. There were six questions posed which deal with whether (i) the organization there has been a good interaction with the study team with the organization (*Good interaction*), (ii) the managers had a chance to comprehend the SVID method (*Comprehension of SVIDT*), (iii) the managers *Learned* [the SVIDT method] *from participation*, (iv) the *Recommendation* were *beneficial*, (v) the *SVIDT method* is considered *beneficial* for the organization (vi) and whether the appreciate the student learning by applying the SVIDT method (*Educational benefits by LAR*).

3. Evaluation and results

We report about a first application of the SVIDT method in the framework of a special form of higher education. Students of the professional Master of Science program of continuing education in management and information technology at Danube University Krems, Austria participated in a course titled *learning by doing applied research* (LAR; German: *Angewandte Lehrforschung*). The subject of this course was the operationalization of the SVIDT method. We present the constraints of the results of the validation of the three modes of the SVIDT method.

3.1. Data acquisition

3.1.1. Study groups

The SVIDT method was applied by 56 students participating in a two-year professional Master of Science program of continuing education in management and information technology. The students chose to collaborate in one of 18 study groups comprised of between two and five members each. According to special admission standards to this master's program, most of the students had no previous bachelor or other academic degree (only 2 of 56). Most of the students, i.e., 38 (68%), earned their certificate to attend the master's course through special practical certificates (e.g., master craftsman in a dual-educational system as a bachelor equivalent) without a senior high school examination. Only 21% of the students were younger than 30 years old; 29% were between 31 and 36 [and 50% were older than 37 years. A strong gender bias was shown, with only 5 of the 56 being women. The study-group members had high profiles in professional expertise; in total, 41% were on the CEO or upper-management level, and 20% were from a lower-management level. The rest were working in technical professions or consulting.

The study-team groups were coached by eight senior coaches. There was at least one manager from each participating organization (called the pivot) involved in the whole course of the study. Depending on the position of the pivot (ranging from department head to CEO), other members of the organization were involved as well.

3.1.2. Organizations

A total of 18 organizations participated in the study; there was no random sampling of the participating organizations. Of the organizations, 12 came from the coaches' network of companies; 6 were (co-)owned by study-team members or employed them. The companies belonged to the categories *business and industry* ($N = 9$; ranging from financial institutions to car parts suppliers), *ICT* companies of various sizes ($N = 6$), and *public organizations* ($N = 3$). For large companies, only departments (e.g., for a car part supplier) were considered.

3.1.3. Constraints of the study

Each member of the study groups worked approximately 250–300 h (including learning and participating in learning the method). The application took place from November 2016 to June 2017.

3.1.4. Data

Each study team gathered data about the organization from the Internet, as well as from data and material that was given to them confidentially by the organization. Each study team wrote a report, including a system model, an assessment of the vulnerability score, and recommendations on how the company should adapt to digital transitioning based on the application of the SVIDT method. Three types of data were selected. *First*, data for understanding and representing the organization, resulting in a quantitative description (number of members, turnover, etc.) were collected. A graphical system representation of the main processes was generated in the course of working through Steps 1 to 4 of the SVIDT method (see Fig. 1). *Second*, all key data of the SVIDT analysis were assessed by the managers of the organization according to detailed interview guidelines, which may be considered the *SVIDT survey tool*. This began with endorsing the Guiding Question (see Step 1; for the following, see Fig. 1); defining the KPIs and weighing their importance; discussing the mission of the company (which includes important information about the weighting between risk avoidance and empowering adaptive capacity); a strength, weakness, and ambiguity table (Step 4); and the impact factors for threat scenarios T_j (Step 6). Then, the students presented three dTC scenarios that they had constructed by themselves, and the managers provided the judgments on the exposure and sensitivity. Then, for one dTC scenario, the managers assessed the adaptive capacity for an intervention scenario $I_{m,j}$ (see Steps 6 and 7). In this step, impact factors $t_{j_n,j}$ and *Consistency scores* for pairwise combinations of levels of impact factors (see Section 2.3) were also assessed by the study team. Finally, the weight between *Risk* and *Adaptive capacity* was assessed. The *Total utility scores*, *Risk*, and *Vulnerability* scores could be calculated based on these data. Probabilities (for *Exposure*, p_j), loss reductions (*Sensitivity*), and weights ($\hat{w}$) were measured on an eleven-level [0,1], graphical Likert-type scale.

Third, an *a posteriori* telephone interview survey was conducted by one member of the team of coaches with managers of all 18 organizations (between 2/18/2017 and 4/9/2017) and with randomly selected members, one from each group (between 11/12/2017 and 12/22/2017). The six questions and the answer scale (a Likert-type scale from 0 to 1) were sent electronically to the participants before the interview. The interviewees first had to provide a quantitative assessment of questions and, afterward, provide comments for all questions. In the post-study evaluation interviews, three questions were examined based on whether *the prerequisites of a thorough SVIDT application were given*. The question *Inclusion* assessed how the application of the *SVIDT survey tool was judged*. How well the managers knew the SVIDT method was appraised by the question labeled *SVIDT*. The degree and value of communication between the study group and the managers was surveyed by the *Interaction* question. The judgments of the question labeled *Meaningful* referred to whether the application of the method provided meaningful recommendations, whereas a follow-up question *(Beneficial)* directly addressed the benefits (utility) for the organization. The last query addressed the question of whether the students and managers appreciated the specific form of LAR as a form of higher education (*Education*).

3.2. Structure validation

The ratings on *Performance, Exposure, Sensitivity, Adaptivity,* and *Normative value* and the composite values, *Risk* and *Vulnerability,* became subjects of an intense exploratory data analysis. The vulnerability score was assessed for the most plausible threat (for a period of doing nothing for three years). Given the time constraints, the judgment was made with respect to one consistent, intuitively plausible scenario. All ratings were normalized to a $[0, 1]$ scale.

Only two judgments on *Exposure* along all variables were potential candidates for statistical outliers (for the Following see Fig. 4). Given a mean of $M = 0.81$, two judgments of an exposure probability of 0.1 and 0.3 were checked. One, the lowest rating, was given for the production department of a well-established automotive parts supplier. The other was for a new (five-year-old) special law firm that provided services on a European level. Due to external basic long-term funding, the exposure and vulnerability ratings were low. Thus, no fundamental inconsistencies could be identified here.

A Kolmogorov–Smirnov test for normal distribution reveals that *Exposure* ($M = 0.81,\ p < 0.001,\ df = 18$) and *Normative value* ($M = 0.29,\ p < 0.003$) do not resemble normal distributions. They are skewed, and a visual analysis suggests a log-normal distribution, with a high *Exposure* value close to 1.

The number of observations was low. Thus, we applied one-factorial ANOVA with Bonferroni post-hoc test in an exploratory manner to identify (potential) differences among the companies. The ICT companies were judged to have a (statistically significant) lower *Sensitivity* (ANOVA: $F = 4.43,\ df = 2,\ p < 0.05$) than the public organizations and also a lower *Risk* (ANOVA: $F = 5.12,\ df = 2,\ p < 0.02$; Bonferroni $p < 0.03$).

The next step explores the correlations among the (formally and statistically contingent) variables. Here, *Sensitivity* and/or *Risk* may be considered as kinds of master variables for on cluster. High Sensitivity correlates significantly with Exposure ($r = 0.64,\ p < 0.02$) with *Adaptive Capacity* ($r = 0.62,\ p < 0.03$) and, thus, naturally with *Risk* ($r = 0.97,\ p < 0.000$). *Vulnerability* is significantly correlated with *Normative value* (i.e., the weighing between *Risk* and *Adaptive Capacity*; $r = 0.70,\ p < 0.001$). This is reflected both by a *Principal Component Analysis* (PCA), resulting in two components along the presented significance of correlation, and by a hierarchical cluster analysis (using Ward's procedure with a squared Euclidian distance; see Fig. 5).

3.3. Validation by organizations - organizations and study-team members' appraisals

All mean judgments of the managers and students were well in the positive domain of the scale (see Fig. 6). A repeated ANOVA measurement on the six validation items of the managers' judgment provided significant differences ($F = 18.80,\ p < 0.001,\ df = 5$). Thus, a Bonferroni post-hoc test provides some results. The appraisal of using SVIDT in a LAR course received the highest rating by far ($M = 9.8$) and significantly higher than the managers' knowledge of SVIDT. Because of the small sample size, no grouping effects were calculated. In total ($N = 116$; two values were missing), only 14% were in the negative range of the scale (i.e., ≤ 5) and only 6% below a rating of 4.

A multivariate analysis utilizing PCA (varimax rotation) reveals that the managers distinguish among three components. The first is whether *SVIDT method* provided *beneficial* results for the *company* (extracting 40% of the variance, based on loadings of > 0.8 for *Beneficial*, *Meaningful*, and knowledge of *SVIDT*), the agreement on SVIDT provides *Educational benefits* when used in *(by) LAR* (extracting 25% of variance), and *Good Interaction*, which may be interpreted as the intensity of involvement of the organization in the study (extracting 20% of variance).

3.4. Validation of the SVIDT application by managers' qualitative judgments

We analyzed the interviews of managers from an SVIDT validation perspective. First, we checked whether the application of the SVIDT was meeting the expectations of the managers and whether

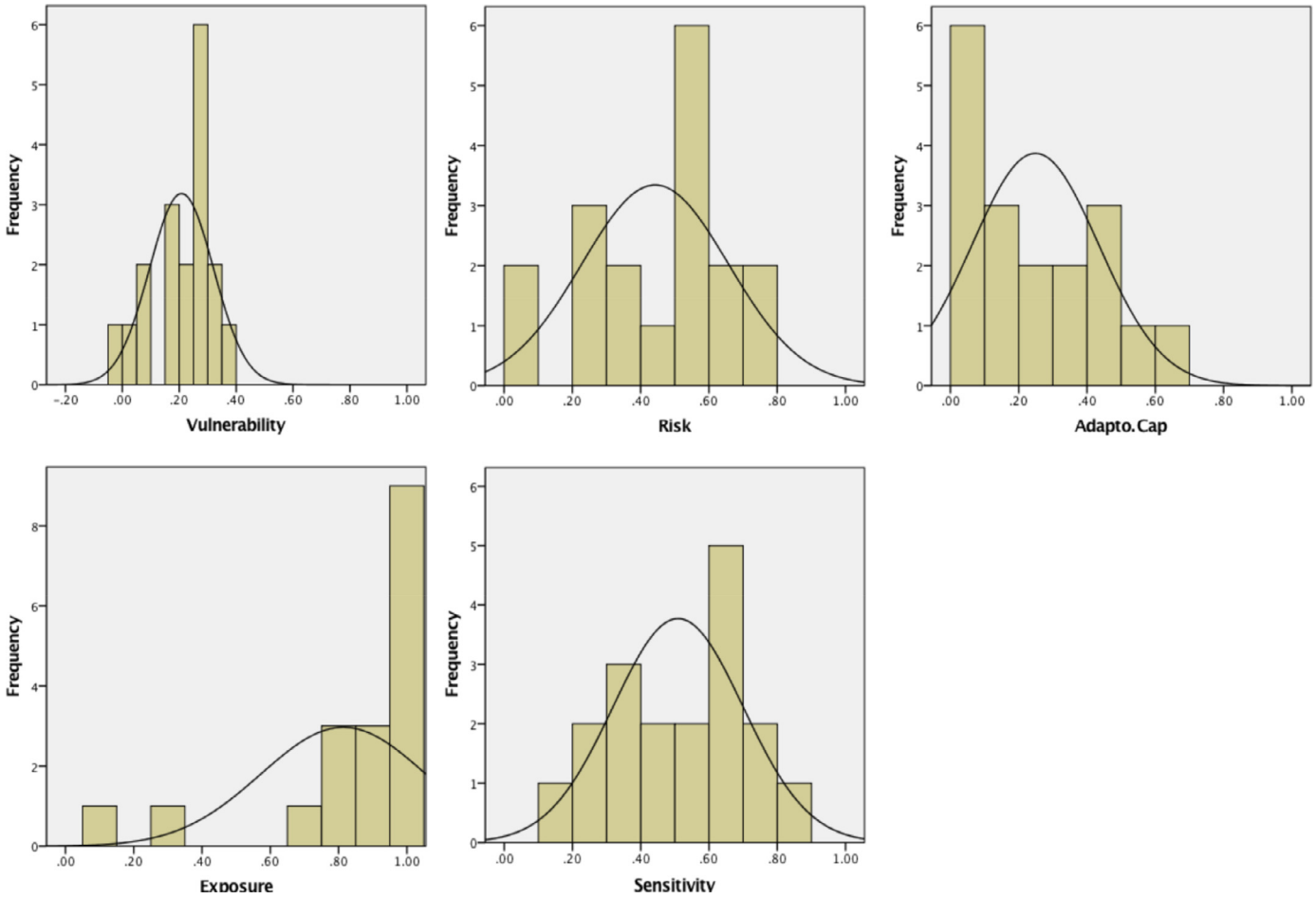

Fig. 4. Frequency distributions for risk, Adaptive capacity ($N = 18$ observations each).

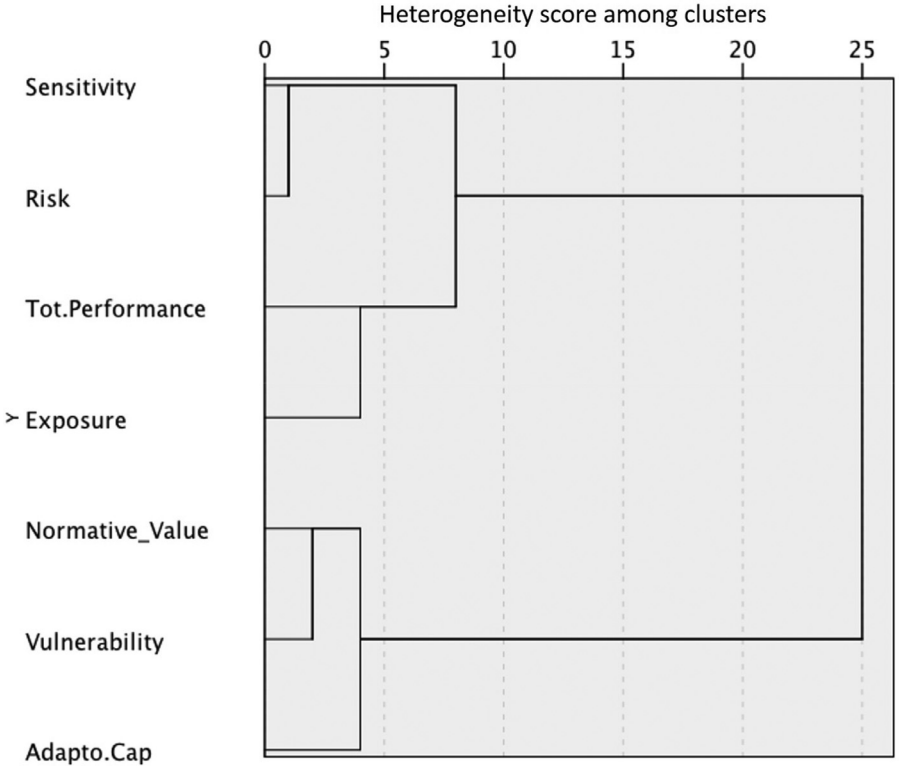

Fig. 5. Cluster analysis in the key scores of the SVIDT method.

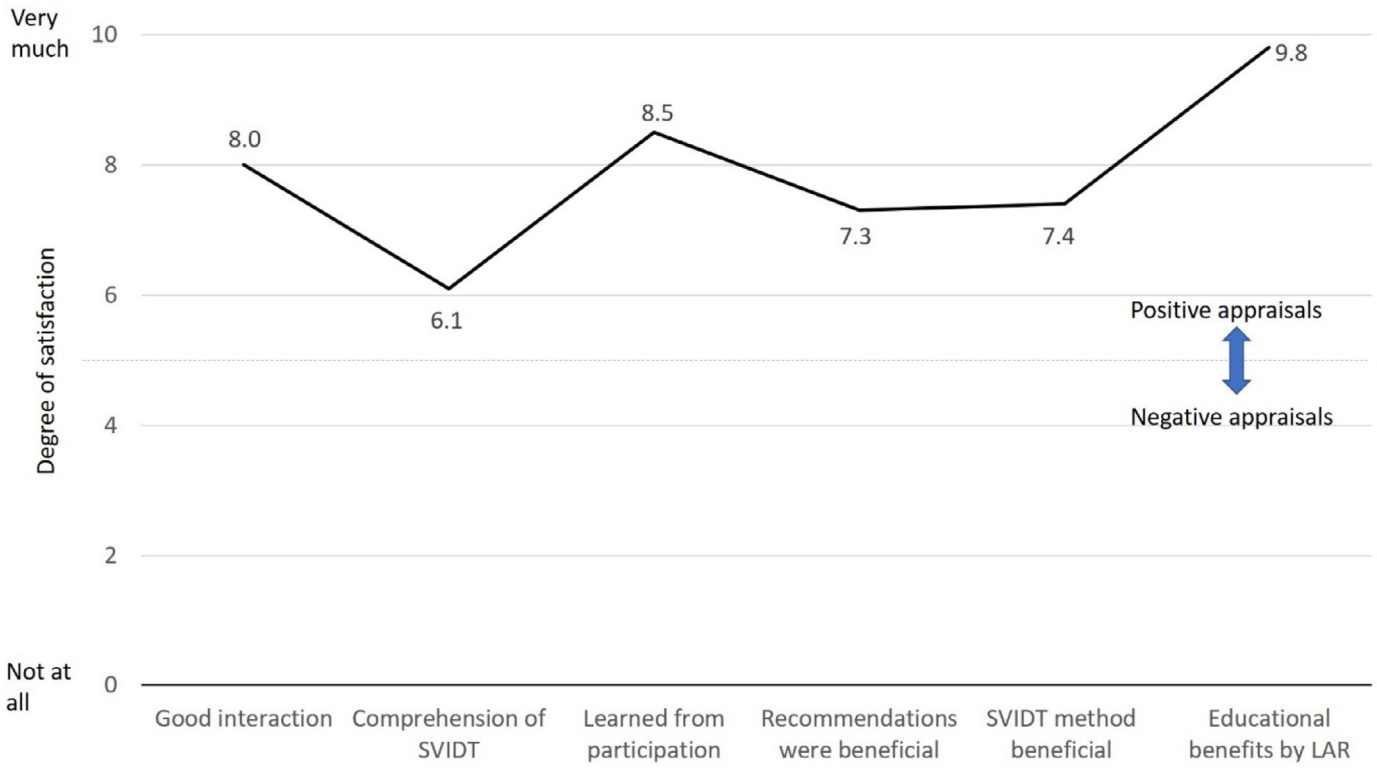

Fig. 6. Mean appraisal judgments of managers on the degree of satisfaction.

SVIDT was sufficiently understood by them. Then we looked at the judgments for *Meaningful* and *Beneficial* (see 3.1.4).

3.4.1. Managers' inclusion and knowledge of SVIDT

The organizations did not mandate the SVIDT analysis but participated voluntarily in an academic LAR course. Despite this and given the high demands on students of continuing education (most are working and combining their family lives and studies are in their leisure time, while simultaneously learning and applying the method), the statements on the inclusion were very positive. All but two (of 18 managers) noted that their inclusion in the project by the team was sufficient and, in some cases, even harmonious.

- *Feel being included quite well.* (Head of Sales of a very large ICT Company)
- *I am excited about the team. They have asked for a lot of information, and they have really used all* [the] *information.* (Production manager for a small production business – SME)

In total, 14 of the 18 managers found that they had at least a basic understanding of the method; they saw SVIDT as helpful for understanding where the company stands in regard to the digital transformation and what strategies they should use to begin adapting to it. Typical statements:

- *As we apply similar methods in our enterprise, SVIDT was easy to understand for me. Otherwise, it is difficult to understand* (Owner and general manager of a small ICT – SME)
- *I looked at the SVIDT method in some detail after the project. Perfect, really good. It fits well.* (Owner and general manager of a small production business – SME)

Examples of a negative statement included the following:

- *I just got marginal access to the method.* (Area manager in public administration for a mid-sized town)
- *I just dealt with the method in a somewhat superficial manner. But it is very interesting. Up to now, I was primarily dealing with the results provided by the team.* (Owner and general manager of a local restaurant chain)

Actually, the judgments on the data collection with the *SVIDT survey tool* are most important, as they refer to the quality of the core data for SVIDT. There were only two ratings by the managers below "8." The qualitative judgments read as follows:

- *In principle, this has been a good interaction. But it would have been better if I had the questions before the interview in order to prepare the answers.* (Owner and general manager of a small ICT – SME)
- *I could answer the questions. Yet, as a manager of the XY company, I would have liked to get some supplementary questions.* (Head of sales for a very large ICT enterprise)

Typical positive answers reveal that the managers were highly challenged but felt that they could answer the quantitative questions:

- *The questions were very good. But it takes time to think about the answers.* (Country manager for a very large ICT enterprise)
- *This was a remarkable talk. From my side, I could have continued for hours. Very interesting. Very precise questions. And absolutely well prepared.* (Production manager of a small production business – SME)

3.4.2. Judgments on the meaningfulness and usefulness of SVIDT method

There were 15 positive and 3 negative statements with respect to whether the recommendations made to the company were meaningful. The positive ones can be divided between those managers who acknowledge that they gained new ideas and those who see their business strategies as confirmed.

- *My view on IoT got partly changed. Yet not everything can be implemented under the given corporate guidelines of our concern. The human resources people have to think differently.* (Head of a regional office of a large ICT)
- *The recommendation fits us 100%. We discussed them together.* (CIO of a large Austrian bank)

An affirming statement read:

- *The recommendations have confirmed what we already knew. We now have a scientific reasoning for this. Consequently, the method shows correctness.* (General manager of a mid-sized production business – SME)

The follow-up question was more general, and the answers partly coincided with the previous one. However, there are two partially contradictory lines of arguments. One involves the "complexity of the subject" and the feeling that "*SVIDT is oversized* for smaller" companies (mid-sized ICT SME, with 120 employees) and not an ideal instrument for small enterprises (small ICT with 5 employees). The other is the decomposition and quantification of vulnerabilities. This is the message of the following statements:

- *[The application of SVIDT has been] Very beneficial. I am going to apply it again. I would like to elaborate the risks and threats in more detail so that the recommendations become 'more significant and valid'.* (Production manager of a small SME – pet-food producer)
- *It is important to translate "feelings" into quantitative numbers. It is much easier to argue in the numerical landscape.* (CIO of a large Austrian bank)

4. Discussion

4.1. Providing a quantitative assessment of vulnerability based on quantitative and qualitative knowledge

The SVIDT method, as operationalized in this paper, is kind of *stress test* and comprehensive *vulnerability assessment*. This may become a management tool for economic and (semi)public organizations when developing strategies to adapt to the challenges of the digital transformation. It provides a quantitative assessment of vulnerabilities and of their major conceptual components, *risk* and *adaptive capacity*. The comprehensive (primarily) *qualitative multilevel system analysis* (see Fig. 1) included the organizational structure and processes, the organization's role and function in the value chain, and a strength and weakness analysis with respect to digital changes as a starting point for constructing dTC scenarios. By means of a thought experiment, the impacts of the dTC scenarios on the key performance indicators were assessed. When constructing intervention scenarios to address selected dTC scenarios, the *adaptive capacity* was operationalized as the organization's potential to compensate prospective losses by increasing its adaptive capacity to digital innovations.

For applying SVIDT, the goals and system boundaries must be unanimously specified. This, as with many other steps, requires the genuine involvement and participation of people within the organization (practice). The primary outcomes of SVIDT are a set of well-selected, coupled threat × intervention scenarios and their quantitative assessments. These allow us to define and prioritize specific digital business strategies and potential collaboration for developing win–win strategies with other actors. The conceptual framework of the method has been described by Scholz (2017a). The present paper provides the application of the method to 18 organizations.

The roots of SVIDT are in *risk and decision analysis* and *problem-structuring methods* including *strategic options management*, but in addition, *transdisciplinary transition management* was mentioned in the introduction and is discussed by Scholz (2017a). The SVIDT method is specifically designed for coping with the *systemic risk of the digital transformation*. This transition is characterized by an extraordinary complexity of interacting systems and entities in all domains of life with – in many domains – unknown speed and impacts (Cox Jr, 2012). And while some knowledge exists, there is also significant ignorance both with respect to specific issues (e.g., when will autonomous vehicles run on highways?) as well as to general issues on the side of human systems that are users of digital technologies (e.g., will there be adverse effects of artificial intelligence in Europe as it spreads with respect to genetically modified organisms?). Against this background, much emphasis has been given to the definition of the *Guiding Question* and the qualitative, structured system analysis that provides basic organizational and contextual data. The complexity of the social actors (e.g., competitors, framing agents) calls, from its very beginnings, for thinking and modeling a multilevel and multi-actor system model (Baudry, Macharis, & Vallée, 2018). We can learn from the presented application that the hierarchy postulate of the HES framework (Scholz, 2011) is extremely helpful, as it helps to differentiate between the drivers and rationales of different human systems (e.g., of individuals, companies, public institutions), which is important for identifying and assessing threats. In some sense, the Guiding Question plays the role of the hypothesis in an experimental study. All project activities have to be functionally related to the Guiding Question. If this relationship is lacking, the coherence of the data falls short, and unnecessary data are produced. Thus, SVIDT is a fully structured, multistep, integrated, hybrid method (and not a "toolbox" from which one may select several tools).

The architecture resembles other methods of risk management, such as the *Failure Mode and Effect Analysis* (FMEA) (Carbone & Tippett, 2004; Stamatis, 2003), which assesses failure risks of products, technologies, projects, etc. The methods used and integrated in SVIDT are presented in Table 1. We do not think that the two parts can be separated. Which digital technologies are relevant for an organization, which actors might contribute to win–win strategies, and the ways in which framing agents might affect the construction of the coupled threat and intervention scenarios and the assessment of their impacts on KPIs is, ultimately, related to a sound system analysis.

Table 1
Methods included in SVIDT.

System Analysis (left part of Fig. 1)	**dTC Scenario and Intervention Assessment** (right part of Fig. 1)
Guiding Question-based project planning	Scenario construction by means of Formative Scenario Analysis for • dTC Scenarios • Intervention Scenarios
Actor analysis: system-based analysis*	Consistency analysis (for dTC and Intervention Scenarios)
Multilevel analysis,* identifying drivers and rationales of a hierarchy of human systems (the HES framework)	Risk assessment (by means of dTC scenarios) • Exposure assessment • Sensitivity assessment
System modeling (for the organization)**	Adaptive capacity assessment
Multicriteria assessment (e.g., of key performance indicators)	Vulnerability assessment • By integrating (weighing) *a priori* risk and *a posteriori* adaptation assessment
Exposure assessment: strengths–weaknesses (SWOT) Analysis	Win–Win analysis

* Drivers and actors are identified according to the hierarchy assumption of the HES framework.

** This is done with the help of impact factors (including impact matrix, impact graph, and impact grid).

We also want to refer to related quantitative assessment of resilience and vulnerability of critical infrastructures. Here, the objective is the construction of proper protection strategies for disruptive events (e.g. natural hazards) or attacks (e.g., cyber-based). Bier and Gutfraind (2019) introduce the concept of defensibility as a basic characteristic of system security. They do this in a very similar manner as we defined the vulnerability concept to compute attack damage before and after defense" (2019, p. 635) and refer to a very similar concepts as components of defensibility than we do for resilience. Also Fang and Zio (2019) stress the importance of post-disruption decision making and provide to bridge the gap between "accurately predicting the hazard information in the classical probability-based analysis and the over conservatism of the pure worst-case" (2019, p. 1121) assessment. The case of natural hazards allows for a more statistical-based approach, yet the conceptual and methodological challenges are very similar as discussed below.

4.2. A "delayed-response stress test" as a key to moving from risk to vulnerability

Conceptually, SVIDT is anchored in *vulnerability and resilience management* (Adger, 2006; Aven, 2007, 2011, 2016; Gheorghe, 2005; Scholz et al., 2012). The focus is on specified resilience as the threat scenarios contain single threats that are more or less known. Formally, the assessment culminates in a quantitative vulnerability score. Historically, risk has been an evaluation function for forthcoming uncertain negative events. Technically, a quantification of risk is usually based on constructing probability distributions and the (outcomes of) negative events for (carefully) selected threat scenarios.

SVIDT does not follow this approach entirely but considers a small set of well-selected dTC scenarios. Special attention has to be paid to the construction of these sets. Digital threats and changes may be viewed as typical systemic risks. Yet, the risks emerging in the digital transition cannot be quantified and may be viewed as typical *systemic risk* (Renn & Klinke, 2004). From a risk-modeling perspective, systemic risk emerges from a multitude – or perhaps better, a myriad – of interacting, interwoven, conditionally contingent (correlated) factors that show feedback of a different order (Renn, Scholz, & Schweizer, 2019). A formal conceptual analysis (Szcesny, 2018) revealed that there were 46 diverse, different, logically and presumably empirically (with respect to their discourse of implementation and use) digital threats (innovations) identified by the study teams across all 18 organizations.

Given these prospects, the key aim of the SVIDT method is to assess vulnerability scores in a thought experiment that can be considered a "delayed-response stress test." This allows the linking of the *a priori* risk perspective and the *a posteriori* adaptive capacity assessments. Experts provided estimates (partly based on numerical empirical data) of the reduction of key performance indicators by a certain dTC scenario and the likelihood that it might become real. Based on this, *a posteriori* view could be taken. The adaptive capacity score had been just the percentage of the loss that could be compensated for after a stand-by period of doing nothing operationally for some time until counteraction was taken to compensate for the postulated loss by a set of interventions, i.e., the intervention scenarios (see Fig. 3B). In the presented application, the experts were the managers of the organizations coached by a study team of student consultants and scientific experts of the digital transition.

We want to stress that the delayed-response evaluation has to be based on a solid foundation. This foundation is a multilevel system analysis (the fundament), which allows the identification of relevant dTCs (the foundation walls) and, subsequently, a small set of significantly different, consistent, impact-factor-based dTC scenarios (the ceiling). A key challenge, then, is to construct the scenarios in such a way that they sufficiently represent the major (possible) directions of future development (in a well-defined time range that has been specified in the Guiding Question). Methodologically, reliability (also from a gentle validation perspective; see Section 2.5) plays an important role in this context. We argue that the highly structured SVIDT process supports the idea that similar (and, ideally, the same) scenarios for one organization may be constructed by different teams (Heugens & van Oosterhout, 2001; Tietje, 2005). Naturally, the question of what threat scenarios have to be constructed depends on the specific organization, the branch, and the degree of development (which differs, e.g., between branches and between developed and developing countries). We argue that the SVIDT process of selecting a few consistent scenarios goes far beyond the common way of looking at worst-case scenarios (Fang & Zio, 2019; Ghaoui, Oks, & Oustry, 2003; Hinkel et al., 2015). In the presented study, the question of which scenarios had to be selected did not cause significant problems. This is partly due to the consistency analysis. Only those scenarios that include meaningful configurations of technologies are considered. Technically, these scenarios included two or three sets (clusters or bundles) of dTCs (i.e., digital technologies that were implemented or had not been implemented) whose development is highly contingent. This is in line with the idea of constructing "plausible scenarios" (Breuer, Jandacka, Rheinberger, & Summer, 2009).

The SVIDT method goes beyond classical risk assessment. Yet, if risk is considered a dynamic process, ideas that resemble a "delayed-response stress test" shine in risk management (McNeil, Frey, & Embrechts, 2015). A common method in financial risk is to look at the value at risk or at the worst-case scenario. We argue that, methodologically, both the way an *a priori* risk assessment and an *a posteriori* adaptive capacity assessment is done and how the dTC intervention scenarios are linked in the "delayed-response stress test" provide new and practically feasible (see Section 3.4) strategies for coping with risks related to the digital transformation as well as other systemic risks. When considering more than one scenario only (such as the worst-case scenario), (subjectively) assessing the likelihood of consistent future scenarios (and the organization's sensitivity, etc.), and then considering the distribution or mean vulnerability scores provides insight into forthcoming adaptations that may be developed.

From an epistemological perspective, if we refer to Egon Brunswik's theory of probabilistic functionalism (Brunswik, 1952), the threat scenarios may be viewed as *cues* (Scholz, 2017b), i.e., sign-significates, which signal essential properties and characteristics of the future digital environment. The challenge is to identify (i.e., to anticipate) those changes, alterations, or transformations (i.e., threats) that sufficiently represent how the world might look like tomorrow and to assist organizations (or other human systems) to adapt to these settings. We assume that, if the reduction of exposure and sensitivity as well the increase of the organization's capability to adapt to these changes is based on properly selected threat scenarios, foundations of *quantitative resilience management* are developed. The interested reader can find a discussion of the epistemological foundations and how this can be done in planning groups in two key papers and eight related comments on the question of the ways in which planning groups may improve their performance when utilizing Brunswik's basic ideas of probabilistic functionalism (see Dedeurwaerdere, 2018; Hoffrage, 2018; Mumpower, 2018; Scholz, 2018; and Steiner, 2018), which can also be applied to essential steps of the SVIDT method.

4.3. A promising first "gentle validation" of a hybrid method

The case of the adaptation of casinos to online gambling has been used as a heuristic case in a previous paper (Scholz, 2017a).

Table 2
Overview of future research regarding practical utility.

No.	Applied method	Identified issues	Reduced practical utility
(1)	Guiding Question-based project planning	Framing the guiding question took several iterations, a hurdle similar to the formulation of mission statements and OKRs in organizations.	None, as the described hurdles are already faced by organizations via, e.g., design thinking approaches. Thus, this has to be an iterative process "in reality" as well.
(2)	Actor analysis: system-based analysis	Few or no issues were identified, as the student consultants had full access to the required information via their company contact (pivot).	None, as companies are aware of their official actors, hierarchy, organizational structure, and key actors for the supply chain.
(3)	Multilevel analysis identifying drivers and rationales of a hierarchy of human systems (the HES framework)	The complexity of HES is high and, therefore, the students kept the external stakeholder analysis on a meta-level.	Low, as a market and competitor analysis is common practice. Yet, a well-performed analysis distinguishes successful from unsuccessful companies and organizations. As reality shows, not all student consultants were able to perform this analysis of goals and drivers of different types of actors well.
(4)	System modeling (for the organization)	The student consultants had some difficulties building the model (network). These were related less to the identification of key entities than to a tendency to overrate the strength of interdependencies, thus increasing the difficulty of identifying critical clusters/centralities.	Low-medium, as this process should be guided from an external party. Information from supply chain documentation can support this process. Yet, sensitivity of departments, etc. can make it difficult to reflect on which ties are important and which are not.
(5)	Multicriteria assessment (e.g., identification of key performance indicators)	Identifying KPIs was not an issue for the student consultants as all of them had experience working with these kinds of indicators in their daily professional environments.	Low, as this information can be obtained from the organization's or company's controlling department. The difficulty lies in the overall judgment of priority and importance of these indicators, as this decision serves as the basis for performance evaluation.
(6)	Exposure assessment: strengths/weaknesses (SWOT) analysis	The students had no issues applying SWOT to assess exposure to dTCs, yet in their first assessments, results tended to be on a high-level perspective only.	Low-medium, as a pure application of SWOT provides a fair but often shallow overview. It is imperative to narrow the application scope and to combine SWOT with at least one other context, e.g., via PEST/PESTLE analysis.
(7)	Scenario construction by means of Formative Scenario Analysis for • dTC scenarios • Intervention scenarios	The students had initial difficulties verbally paraphrasing their dTC scenarios. When they had more experience doing so, the results became comprehensive. Especially regarding the intervention scenarios, the students became highly innovative.	Low-medium, as it is impossible to assign a reasoned probability function to the created scenarios; the consistency of dTC scenarios plays an important role. If this successive step is omitted or performed improperly, the risk assessment is negatively affected.
(8)	Consistency analysis (for dTC and Intervention scenarios)	Due to their experience and IT background, the students were able to identify consistency problems with no remarkable issues.	Low, as it becomes an issue only if the required know-how regarding technology and digitalization/digital transformation is missing.
(9)	Risk assessment (by means of dTC scenarios) • Exposure assessment • Sensitivity assessment	While the students had fewer issues in regard to the framing of the general exposure and sensitivity, some groups struggled with the quantification of these. Also, some of the pivots/CIOs of the companies were often uncertain in this regard.	Low-medium, as expert judgment again is the basis for this analysis. While quantitative values might be gathered from existing risk management data, likelihood and time of impact for a dTC still present an uncertainty that cannot be ruled out easily.
(10)	Adaptive capacity assessment	Student consultants had initial issues in regard to quantification of the adaptive capacity of the organization or company under review. The combination of dTC and intervention scenario helped significantly in the dialog with the pivot to finally reach a decision.	Medium, not because the adaptive capacity is inappropriate, but because of the inherent danger of companies/organizations overestimating their own capabilities. Also, if no dTC scenario has occurred (or identified as having occurred), an initial judgment may be difficult.
(11)	Vulnerability assessment by integrating (weighing) a priori risk and a posteriori adaptation assessments	For the student consultants, this was done by a qualitative ranking of the calculated scores, which demonstrated no issues per se.	Low-medium, as the ranking via the calculated scoring may seem fairly "easy," but the final selection of potential high-risk scenarios is a crucial step. Also, if certain scenarios are ranked closely together based on their scoring, judgment and final selection definitely represent a C-level decision.

The present paper has provided a complete operationalization of the parameters and a first validation when applying the SVIDT method to 18 organizations. This became possible through an innovative master course following the *learning by doing applied research* (LAR) principle. This offered the unique opportunity to apply the method under conditions that met many of the criteria for a controlled experiment. All teams carefully went through all nine steps of the method, and the same data were applied for the system analysis. The same questionnaire guide was used to assess the basic expert judgments, and the same software tools were used to assess the consistency scores and to calculate the risk and vulnerability scores. Competent coaching by the staff scientists ensured that the data could be compared. This is why we described the constraints of the application in some detail.

There were several suboptimal issues in the application. For instance, we had groups of student consultants who all had professional experience but did not yet have full-fledged competence as senior researchers or consultants. The post-study interviews with the managers can be considered a kind of quality control. The results (see the answers on the SVIDT tool, in particular, the responses to *Inclusion*, Fig. 6) provided sufficiently good information. Due to time constraints, the (different steps of the) SVIDT method was not ideally conveyed (in detail) to all but the major share of managers. We expected that this would improve the reliability of the data and the recommendations. For the same reason, a structure analysis of the expert judgments and of the composite score was conducted. The distributional analysis provided reasonable results, in particular when showing empirically that *risk* (which is

strongly related to *sensitivity*) and *adaptive capacity* must be considered as two components of resilience management (see Fig. 5). This closely aligns with the results of a previous empirical study (Moser, Stauffacher, Blumer, & Scholz, 2015) that revealed that the adaptive capacity represents aspects different from the risk related to hazardous technological waste (or other threats).

The quantitative assessments and comments of the managers (several months after the study was conducted) proved that the presented study provided a serious application of the SVIDT method that was praised as having provided beneficial results to most of the included organizations. Thus, the SVIDT method has a high potential for practical application, not only as a research instrument for better understanding how the risk and vulnerability of digital changes and threats for organizations can be better understood from a science perspective.

4.4. Needs for further research

We identified several issues that call for some elaboration and future research. Conceptually and methodologically, two issues require further development. One is the *selection of the dTC scenarios* and the construction of an integrative vulnerability score. Tietje (2005) developed a method for selecting a small set of significantly different scenarios (which was implicitly applied by the coaching team when selecting the scenarios). Work such as that by Borgonova and Plischke (2016) discuss the approach in the context of the sensitivity analysis of risk assessment (see also (Mazzorana, Hübl, & Fuchs, 2009). The constraints of the LAR course did not allow for an elaboration of this aspect in the presented study. Therefore, further empirical, conceptual, and theoretical investigations are needed.

We also expect that the selection of single threats can be improved in reference to Brunswik's concept of cues. This may refer primarily to the selection of single threats. This has to be done in a balanced manner as "too many similar and correlated" risks affect the consistency scores and the selection of the threat scenarios and, thereby, ultimately the risk and vulnerability scores. The cue concept (Brunswik & Kamiya, 1953; Scholz, 2018) suggests selecting a few, partially overlapping and partly substitutable cues that satisfyingly provide a reliable assessment about potential states of environments. A further issue that call for conceptual development is the complementarity between the *a priori* risk and *a posteriori* vulnerability management. This becomes of special interest if the costs of continuous information acquisition and for risk management and building adaptive capacity are quantitatively modeled and assessed.

In order to provide further insights to managers and researchers contemplating the use of the SVIDT, we summarized the applied methods, identified issues, and potential reductions of practical utility in Table 2. By doing so, we offer starting points for practitioners as well as researchers regarding future optimization, customization, and extension of SVIDT, also in regard to the currently included methods, to be able to further increase portability of SVIDT to other sectors and application domains.

4.5. Relating soft operational methods and common methods of operational research

Historically, the systems approach, complexity theories, and problem structuring methods complemented mathematical and computer modeling approaches already since the nineteen sixties (see e.g., Ackoff, 1962; Mingers & White, 2010). One reason was that the prerequisites of applying quantitative approaches were not meeting the complexity, e.g., of the organizations' environment or internal processes (Mintzberg, 1994). The soft systems methodology, primarily promoted by British operational researchers (Rosenhead, 2009) stressed the qualitative side and has not been really overcome the gap to mainstream operational research as you may take from a contemporary operations research and management science handbook (Ravindran, 2008). The presented SVIDT method is a hybrid method. This is uncommon for mainstream operational research. But, it allows both the acknowledging to the sometimes perplexing uncertainty (Rosenhead, 1998) of the organization challenge to cope with adaptations to a digital world and to utilize profound formal and quantitative approaches from operational research. The sophisticated construction of threat scenarios (overcoming simplified worst case analysis) for the digital transition, the – partly quantitative analysis-based expert judgements of losses by dTC scenarios – or judgments on the compensating effect of intervention scenarios on the organizations' key performance indicators may be taken as example. Thus, SVIDT can be considered as a comprehensive problem structuring framework which allows to utilize formal and quantitative methods of mainstream operational research (see, e.g. (Ravindran, 2008)) such as multicriteria decision analysis (Masud & Ravindran, 2008), or scenario based decision analysis (Klein, 2008; Wright, Cairns, O'Brien, & Goodwin, 2018). This has been done when assessing quantitative vulnerability scores, based on thoroughly constructed and selected threat and intervention scenarios, while also including the important aspect of uncertainty from a future viewpoint (see Wright et al., 2018). Thus, SVIDT may be seen as an example of relating soft operational methods and common methods of operational research.

5. Conclusions

Digital threats and changes can be conceived as a certain type of systemic risk as they emerge from a multitude of interacting, interwoven, multilevel, conditionally contingent (correlated) change factors (threats) that take place at different levels of society. This setting does not allow for the construction of risk scores in a common manner. Based on a highly structured multilevel system analysis, SVIDT provides a hybrid method for constructing a small set of consistent, significantly different dTC scenarios and related consistent intervention scenarios. Based on this, the SVIDT method quantifies risk and adaptive capacity as key components of vulnerability by expert assessments of sensitivity, exposure, and adaptive capacity. Given weighing whether adaptive action can and/or should be taken before a negative event takes place or whether a post-negative-event adaptation is preferred, the method provides a quantitative vulnerability assessment and allows organizations to compare and to select intervention strategies.

A first empirical application of SVIDT to 18 organizations in Austria and Germany worked remarkably well. The managers of the organizations acknowledged the method, its potential, and mostly the beneficial impacts of participating in the process of applying SVIDT and receiving recommendations. Thus, the skepticism that an integrated method such as SVIDT may be too complex for practice has vanished. By contrast, vulnerability scores depend on the choice and construction of dTC and intervention scenarios, and these, in turn, are based on which threats are chosen; this is an impact of the system and strengths and weaknesses analysis. We may learn from this that the investigation of highly complex – and, at first glance, unstructured issues such as the assessment of digital risks and vulnerabilities – from a highly structured, hybrid method such as the SVIDT method has significant potential and value.

Acknowledgments

We want to thank 18 organizations and their CEOs and managers to participate in the SVIDT application, 56 students of the

Danube University of continuing education for their exceptional commitment when applying the SVIDT method, Günther Schrader and Sören W. Scholz for their valuable feedbacks and Elaine Ambrose for her insightful English editing of the text. Regarding the sequence of authors, the FLAE norm was applied.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ejor.2019.09.020.

References

Ackermann, F. (2012). Problem structuring methods 'in the dock': arguing the case for soft or. *European Journal of the Operational Research, 219*(3), 652–658. doi:10.1016/j.ejor.2011.11.014.

Ackoff, R. L. (1962). Some unsolved problems in problem solving. *Journal of the Operational Research Society, 13*(1), 1–11.

Adger, W. N. (2000). Social and ecological resilience: are they related. *Program Human Geography, 24*, 347–364.

Adger, W. N. (2006). Vulnerability. *Global Environmental Change, 16*(3), 268–281. Retrieved from http://www.sciencedirect.com/science/article/B6VFV-4KFMM81-2/2/22ffaffffa0ef5f8451decd3ed9240c3.

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety, 92*(6), 745–754. doi:10.1016/j.ress.2006.03.008.

Aven, T. (2011). On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis, 31*(4), 515–522. doi:10.1111/j.1539-6924.2010.01528.x.

Aven, T. (2016). Risk assessment and risk management: review of recent advances on their foundation. *European Journal of the Operational Research, 253*(1), 1–13. doi:10.1016/j.ejor.2015.12.023.

Baudry, G., Macharis, C., & Vallée, T. (2018). Range-based multi-actor multi-criteria analysis: A combined method of multi-actor multi-criteria analysis and monte carlo simulation to support participatory decision making under uncertainty. *European Journal of the Operational Research, 264*(1), 257–269.

Bier, V., & Gutfraind, A. (2019). Risk analysis beyond vulnerability and resilience - characterizing the defensibility of critical systems. *European Journal of the Operational Research, 276*(2), 626–636. doi:10.1016/j.ejor.2019.01.011.

Bojanova, I. (2014). *The digital revolution: What's on the horizon?* IT Pro (pp. 8–12) February.

Borgonovo, E., & Plischke, E. (2016). Sensitivity analysis: A review of recent advances. *European Journal of the Operational Research, 248*(3), 869–887.

Brachinger, H. W., & Weber, M. (1997). Risk as a primitive: A survey of measures of perceived risk. *Operations Research-Spectrum, 19*(4), 235–294.

Breuer, T., Jandacka, M., Rheinberger, K., & Summer, M. (2009). *How to find plausible, severe, and useful stress scenarios*. Österr: Nationalbank.

Brunswik, E. (1952). *The conceptual framework of psychology*. Chicago, IL: University of Chicago Press.

Brunswik, E., & Kamiya, J. (1953). Ecological cue validity of 'proximity' and of other Gestalt factors. *American Journal of Psychology, 66*, 20–32.

Brynjolfsson, E., & McAfee, A. (2012). *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy*. Brynjolfsson and McAfee.

Carbone, T. A., & Tippett, D. D. (2004). Project risk management using the project risk FMEA. *Engineering Management Journal, 16*(4), 28–35.

Checkland, P., & Scholes, J. (1990). *Soft systems methodology in action*. Chichester: Wiley.

Courtland, R. (2015). Gordon Moore: the man whose name means progress. Gordon Moore: the man whose name means progress. *IEEE Spectrum. March 30, 2015*. Retrieved from http://spectrum.ieee.org/computing/hardware/gordon-moore-the-man-whose-name-means-progress.

Cox, L. A. Jr (2012). Confronting deep uncertainties in risk analysis. *Risk Analysis, 32*(10), 1607–1629.

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin, 52*, 281–302.

Dedeurwaerdere, T. (2018). From ecological psychology to four varieties of post-positivism in transdisciplinary science. Comment on "Contributions to Brunswik's Theory of Probabilistic functionalism". Environment Systems and Decisions

Dyson, R. G. (2004). Strategic development and swot analysis at the University of Warwick. *European Journal of the Operational Research, 152*(3), 631–640.

Eden, C., & Ackermann, F. (2006). Where next for problem structuring methods. *Journal of the Operational Research Society, 57*(7), 766–768. doi:10.1057/palgrave.jors.2602090.

Eden, C., & Huxham, C. (2006). Researching organizations using action research. In S. R. Clegg, C. Hardy, T. B. Lawrence, & W. D. Nordhaus (Eds.), *The SAGE handbook of organization studies* (pp. 388–408). Los Angeles, CA: Sage.

Eden, C., & Smithin, T. (1979). Operational gaming in action research. *European Journal of the Operational Research, 3*(6), 450–458. doi:10.1016/0377-2217(79)90028-6.

Einhorn, H. J., & Hogarth, R. M. (1986). Decision-making under ambiguity. *Journal of Business, 59*(4), S225–S250 Retrieved from <Go to ISI>://A1986F015300004.

Fang, Y.-P., & Zio, E. (2019). An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards. *European Journal of the Operational Research*.

Friend, J., & Hickling, J. (2005). *Planning under Pressure. The strategic choice approach*. Amsterdam: Elsevier.

Ghaoui, L. E., Oks, M., & Oustry, F. (2003). Worst-case value-at-risk and robust portfolio optimization: A conic programming approach. *Operations Research, 51*(4), 543–556.

Gheorghe, A. V. (Ed.). (2005). *Integrated risk and vulnerability management assisted by decision support systems: Relevance and impacts on governance*. Dordrecht, NL: Springer.

Gottschalk, F., Scholz, R. W., & Nowack, B. (2009). Probabilistic material flow modeling for assessing the environmental exposure to compounds: methodology and an application to engineered nano-TiO2 particles. *Environmental Modeling & Software, 25*, 320–332.

Götze, U. (1990). *Szenario-Technik in der strategischen Unternehmensplanung* (2nd ed.). Wiesbaden: Deuscher Universitäts Verlag.

Harris, Z. S. (1954). Distributional structure. *Word, 10*(2–3), 146–162.

Helbing, D. (2015). *The Automatization of Society is Next*. Great Britain (Amazon): Dirk Helbing.

Helms, M. M., & Nixon, J. (2010). Exploring swot analysis–where are we now? A review of academic research from the last decade. *Journal of Strategy and Management, 3*(3), 215–251.

Heugens, P. M. A. R., & van Oosterhout, J. (2001). To boldly go where no man has gone before: integrating cognitive and physical features in scenario studies. *Futures, 33*(10), 861–872.

Hinkel, J., Jaeger, C. C., Nicholls, R. J., Lowe, J., Renn, O., & Peijun, S. (2015). Sea-level rise scenarios and coastal risk management. *Nature Climate Change, 5*(3), 188.

Hisrich, R. D., & Ramadani, V. (2017). *Effective entrepreneurial management*. Cham: Springer.

Hoffrage, U. (2018). From representation via planning to action: an extension of Egon Brunswik's Theory of Probabilistic Functionalism. *Environment Systems and Decisions, 38*(1), 69–73.

Hogarth, R. M., & Kunreuther, H. (1985). Ambiguity and insurance decisions. *American Economic Review, 75*(2), 386–390.

Ivanschitz, B.-P., Lampoltshammer, T. J., Mireles, V., Revenko, A., Schlarb, S., & Thurnay, L. (2018). A data market with decentralized repositories. In *Proceedings of the paper presented at the 2nd Workshop on Decentralizing the Semantic Web co-located with the 17th International Semantic Web Conference (ISWC 2018)* October 8, 2018.

Kahneman, D., & Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Econometrica, 47*(2), 263–291.

Keeney, R. L., & Raiffa, H. (1976). *Decisions with multiple objectives: Preferences and value trade-offs*. New York, NY: Wiley.

Klein, C. M. (2008). Decision analysis. In A. R. Ravindran (Ed.), *Operations Research and Management Science Handbook*. CRC Press (pp. 6.1-5.29).

Lang, D. J., Scholz, R. W., Binder, C. R., Wiek, A., & Stäubli, B. (2007). Sustainability potential analysis (SPA) of landfills - a systemic approach: theoretical considerations a systemic. *The Journal of Cleaner Production, 15*(17), 1628–1638. doi:10.1016/j.jclepro.2006.08.004.

Limpert, E., Stahel, W. A., & Abbt, M. (2001). Log-normal distributions across the sciences: Keys and clues. *Bioscience, 51*(5), 341–352 Retrieved from <Go to ISI>://000169293900007.

Masud, A. S. M., & Ravindran, A. R. (2008). Multiple criteria decision making. In A. R. Ravindran (Ed.), *Operations research and management science handbook*. CRC Press (pp. 5.1-5.35).

Mazzorana, B., Hübl, J., & Fuchs, S. (2009). Improving risk assessment by defining consistent and reliable system scenarios. *Natural Hazards and Earth System Sciences, 9*(1), 145–159.

McAfee, A., & Brynjolfsson, E. (2017). *Machine, platform, crowd: Harnessing our digital future*. New York, NY: WW Norton & Company.

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools-revised edition*. Princeton University Press.

Mingers, J. (2000). An idea ahead of its time: the history and development of soft systems methodology. *Systemic Practice and Action Research, 13*(6), 733–755. doi:10.1023/a:1026475428221.

Mingers, J., & Rosenhead, J. (2004). Problem structuring methods in action. *European Journal of the Operational Research, 152*(3), 530–554.

Mingers, J., & White, L. (2010). A review of the recent contribution of systems thinking to operational research and management science. *European Journal of the Operational Research, 207*(3), 1147–1161.

Mintzberg (1994). *The rise and fall of strategic planning: Reconceiving roles for planning, plans, planners*. New York: The Free Press.

Missler-Behr, M. (1993). *Methoden der Szenarioanalyse (Methods of scenario analysis)*.

Moser, C., Stauffacher, M., Blumer, Y. B., & Scholz, R. W. (2015). From risk to vulnerability: the role of perceived adaptive capacity for the acceptance of contested infrastructure. *Journal of Risk Research, 18*(5), 622–636. doi:10.1080/13669877.2014.910687.

Osterwalder, A., & Pigneur, Y. (2010). *Business model generation: A handbook for visionaries, game changers, and challengers*. John Wiley & Sons.

Paustenbach, D. J. (Ed.). (2002). *Human and ecological risk assessment. Theory and practice*. New York, NY: Wiley.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64–88 Retrieved from <Go to ISI>://WOS:000353732700019.

Ravindran, A. R. (Ed.). (2008). *Operations research and management science handbook*. CRC Press.

Reibnitz, V. U. (1992). *Szenario-technik. instrumente für die unternehmerische und persönliche Erfolgsplanung [Scenario technique: Instruments for the enterprising and personal success plan]* (2nd ed.). Wiesbaden: Gabler.

Renn, O., & Klinke, A. (2004). Systemic risks: a new challenge for risk management: As risk analysis and risk management get increasingly caught up in political debates, a new way of looking at and defining the risks of modern technologies becomes necessary. *Embo Reports, 5*(1S), S41–S46.

Rosenhead, J. (1998). Complexity theory and management practice. *Science Culture (London), 19*. Retrieved from http://human-nature.com/science-as-culture/rosenhead.html.

Rosenhead, J. (2006). Past, present and future of problem structuring methods. *Journal of the Operational Research Society, 57*(7), 759–765 Retrieved from <Go to ISI>://WOS:000238385600002.

Rosenhead, J. (2009). Reflections on fifty years of operational research. *Journal of the Operational Research Society, 60*(sup1), S5–S15.

Saaty, T. L., & Ergu, D. (2015). When is a decision-making method trustworthy? Criteria for evaluating multi-criteria decision-making methods. *International Journal of Information Technology & Decision Making, 14*(6), 1171–1187. doi:10.1142/s021962201550025x.

Scholz, R. W. (2011). *Environmental literacy in science and society: From knowledge to decisions*. Cambridge: Cambridge University Press.

Scholz, R. W. (2017a). Digital threat and vulnerability management: the SVIDT method. *Sustainability, 9*(4), 554 ARTN 55410.3390/su9040554.

Scholz, R. W. (2017b). Managing complexity: from visual perception to sustainable transition management. contributions of Brunswick's theory of probabilistic functionalism. *Environment Systems and Decisions, 37*(4), 381–409.

Scholz, R. W. (2017c). The normative dimension in transdisciplinarity, transition management, and transformation sciences: New roles of science and universities in sustainable transitioning. *Sustainability, 9*(991). doi:10.3390/su9060991.

Scholz, R. W. (2018). Ways and modes of utilizing Brunswik's theory of probabilistic functionalism: new perspectives for decision and sustainability research. *Environment Systems and Decisions, 38*(1), 99–117.

Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., & Viale Pereira, G. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. *Sustainability, 10*(6), 2001. doi:10.3390/su10062001.

Scholz, R. W., Blumer, Y. B., & Brand, F. S. (2012). Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective. *Journal of Risk Analysis, 15*(3), 313–330. doi:10.1080/13669877.2011.634522.

Scholz, R. W., & Hansmann, R. (2007). Combining experts' risk judgments on technology performance of phytoremediation: self-confidence ratings, averaging procedures, and formative consensus building. *Risk Analysis, 27*(1), 225–240. doi:10.1111/j.1539-6924.2006.00871.x.

Scholz, R. W., Lang, D. J., Wiek, A., Walter, A. I., & Stauffacher, M. (2006). Transdisciplinary case studies as a means of sustainability learning: historical framework and theory. *International Journal of Sustainability in Higher Education, 7*(3), 226–251.

Scholz, R. W., & Steiner, G. (2015). The real type and the ideal type of transdisciplinary processes. Part II - What constraints and obstacles do we meet in practice? *Sustainability Science, 10*(4), 653–671. doi:10.1007/s11625-015-0327-3.

Scholz, R. W., & Tietje, O. (2002). *Embedded case study methods: Integrating quantitative and qualitative knowledge*. Thousand Oaks, CA: Sage.

Sczesny, L. (2018). *Organisational threat taxonomy — model for classification of threats and changes. Introduction of the OTT model and OTT algorithm as a means for classification of digital threats and changes*. Krems: Danube University of Krems.

Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution*. ASQ Quality Press.

Steiner, G. (2018). From probabilistic functionalism to a mental simulation of innovation: by collaboration from vulnerabilities to resilient societal systems. *Environment Systems and Decisions, 38*(1), 92–98.

Sugiyama, M., Deguchi, H., Ema, A., Kishimoto, A., Mori, J., Shiroyama, H., & Scholz, R. W. (2017). Unintended side effects of digital transition: Perspectives of Japanese experts. *Sustainability, 9*(12) ARTN 219310.3390/su9122193.

Tietje, O. (2005). Identification of a small reliable and efficient set of consistent scenarios. *European Journal of the Operational Research, 162*(2), 418–432.

Velik, R. (2010). Quo vadis, intelligent machine? *BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 1*(4), 13–22.

Wallerstein, N., & Duran, B. (2010). Community-based participatory research contributions to intervention research: the intersection of science and practice to improve health equity. *American Journal of Public Health, 100*, S40–S46. doi:10.2105/ajph.2009.184036.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud computing–a classification, business models, and research directions. *Business & Information Systems Engineering, 1*(5), 391–399.

Wright, G., Cairns, G., O'Brien, F., & Goodwin, P. (2018). Scenario analysis to support decision making in addressing wicked problems: Pitfalls and potential. *European Journal of the Operational Research, 278*(1), 3–19.