Panarchy Process for Risk Control and Resilience Quantification and Improvement

Ivo Häring, Sebastian Ganter, Jörg Finger, Kushal Srivastava

Fraunhofer EMI, Germany. E-mails:
{ivo.haering; sabastian.ganter; joerg.finger; kushal.srivastava}@emi.fraunhofer.de

Evita Agrafioti

Gap Analysis, Crete, Greece. E-mail:
agrafioti@gapanalysis.gr

Clemente Fuggini, Fabio Bolletta

RINA Consulting, Rozzano, Italy. E-mails:
{clemente.fuggini; fabio.bolletta}@rina.org

Risk control based on risk (semi) quantification has much improved, being in many domains by now an auditable, certifiable and insurable process with high economic, ecological and societal relevance. At the same time, the insight has grown that such classical risk management focusing on five-phase risk and chance management is not sufficient to handle major disruptions, unexpected or even unexampled events. In this context, a concept based on catastrophe management and related (technical) capabilities, e.g. within the temporal and logical cycle phases preparation, prevention, protection, response, recovery, and learning, and related resilience concepts, proved to be a successful new and additional approach. However, now the question arises whether classical risk management (thesis) and resilience engineering (antithesis) can be combined within a synthesis, to leverage the rich insights of both approaches. The paper explores the options of combining a risk and resilience management cycle with a resilience cycle within a panarchy loop to achieve a holistic phased and iterative approach. Options are discussed and the best option is selected in terms of orthogonality of phases, merge and limitation of phases, well-defined core tasks of each phase and supporting methods. For the application domain critical infrastructure protection and the industry sector gas, it is shown how to support the phases of the joint risk and resilience management panarchy with the method quantitative gas grid simulation.

Keywords: Panarchy process, resilience analysis and assessment, risk analysis and management, resilience engineering, resilience quantification.

1. Introduction

Quite general, when addressing how to ensure that systems are safe and secure, two options are available. An analytical assessment approach based on system knowledge and an approach based on processes in case of unintended events. A further fundamental distinction often made is between control of unintended events and improvement of desirable behavior in case of known and unknown disruption events.

Classical risk analysis and management can be considered as a blue print for an analytical assessment of unintended events. It can also be considered as a process that is applied qualitatively as an undesired event unfolds for analyzing what to do. Also, to assess chances on objectives. However, its main focus is analytical in-depth analysis and control of unintended events taking account of all risk control and mitigation measures already taken to assess overall acceptability of known risks of systems.

Unintended events include natural hazards, system failures, e.g. due to aging and command failures, accidents, acts of sabotage, and terrorism.

Crisis response management or disruption handling is a process that helps to deal with threats that actually occur, e.g. loss of control of autonomous machinery or supply line subsystem. It can also be used to analyze the technicaland organizational capabilities already in place for managing disruptions. Also, for a better risk and likelihood assessment by assessing the capabilities for phases before, during and after the event. However, the initial focus is on the better actual doing in case of disruptions and related (technical) capabilities rather than deficits.

The question arises whether both approaches can be combined. At the one hand side the analytical assessment approach on the other hand side the action-oriented approach. On the one hand the failure focused approach on the other the capability oriented approach. On the one hand the assessment of known damage events, on the other hand the assessment of novel unexampled threats, e.g. in terms of their effects only.

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0_4264-cd

Besides the conceptual challenge, also the question arises whether the two respective research directions or communities and terminologies may be combined to harness the richness of both approaches. Often in contrast to classical risk analysis and management, the term resilience engineering has been coined and used to describe the process and capability focused approach (Hollnagel et al. 2006). However, by now both communities use well-established concepts, process schemes and methods, hence the question arises how to take advantage of both approaches while avoiding redundancies.

The article asks whether it is conceptionally sound and how it is efficiently feasible to combine the typical circular schemes used for risk assessment (risk or resilience assessment loop) and the crisis or resilience handling cycle. The ambition is to use a combination that contains on first sight (within a one-dimensional black-and white scheme) the main steps of both approaches, while avoiding redundancies as far as possible.

The aim of the article is to first better characterize analytical risk and resilience assessment processes (section 2) as well as disruption management for socio-technical systems (section 3) from an engineering perspective using circular assessment schemes. Section 4 explores whether panarchy (infinity loop) schemes used in the context of socio-ecological resilience research offer a straightforward interpretation for the present context, i.e. support on combining or rearranging the established steps or phases of the assessment and action cycles.

Section 5 looks at different feasible combinations of the assessment cycle and the disruption management cycle using a panarchy. They are discussed and advantages and disadvantages are listed. For the preferred panarchy topology and steps definitions, section 6 provides as example the applicability of the method model-based simulation to large-scale gas grid critical infrastructure to illustrate the panarchy resilience process and how it links to methods, techniques and measures. Section 7 concludes by summarizing the main arguments used and discusses further challenges.

2. Circles for Risk and Resilience Analysis

The classical five-step risk analysis has been standardized in ISO 31000 2018 and by now several domain-specific application standards are available including compliance and environmental management standards (Lalonde and Boiral 2012). In the technical domain, all functional safety standards based on IEC 61508, 2010 conduct hazard and risk analyses resorting to a consideration of frequencies (probability) and probability measures for assessing risks of systems.

Most often the process shown in

Fig. *1* is used, conducted within a framework and by applying principles (Olechowski et al. 2016).

Fig. 1. Risk cycle process: 5-step risk analysis and management process according to ISO 31000 (2018) clause 6.

Risk analysis and management focuses mainly on the prevention of unintended events, however, in some cases, this cannot guarantee an efficient overall risk control. For instance, when dealing with complex systems that are characterized by great uncertainties, the typical probabilistic risk analysis and assessment appears to have limitations (Aven 2019). To this end, performance based-resilience, which is related to the ability to regain/store systems' performance upon a change in condition or an event occurrence (either known or unknown) (Thekdi and Aven 2019), needs to be also considered.

In the literature several approaches have been proposed for performance-based resilience management which include (extensions of) risk management as a special case. In terms of this broad resilience management approaches and terminology, risk management focuses on the reduction of the frequency of events (prevention, reduction of susceptibility) and the increase of robustness (decrease of initial damage, decrease of vulnerability, better absorption).

A sample process that can be conducted analytically or by using quantitative performance functions is provided in (Häring et al. 2017). It is compliant with ISO 31000 (2018) and can be tailored, in particular to the telecommunication domain (Fehling-Kaschek et al. 2019), see Fig. 2.

Resilience management in a narrower sense focuses on improving system behavior post disruption events. That is on reducing the system performance loss time, on increasing its recovery slope and on achieving as fast as possible the initial performance or even increasing the final performance when compared to the initial system performance, and similar objectives.

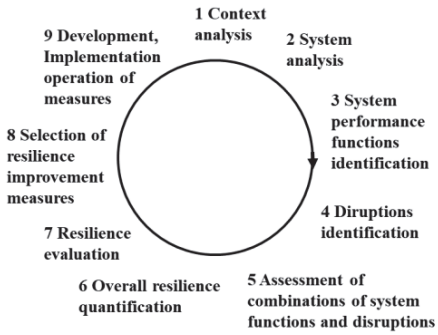

Fig. 2. Joint risk and resilience cycle: 9-step system performance-function based resilience analysis and management conformal with ISO 31000, according to (Häring et al. 2017).

An advantage of the process given in Fig. 2 is that it can be conducted qualitatively as well as semi-quantitatively and quantitatively (in particular step 6). Furthermore, that it is focusing on system performance quantities, which can also be identified or linked to key performance indicators (KPI) of a system. A disadvantage is that is does not use the well-known risk cycle (see Fig. 1) and resilience cycle (see Fig. 5) explicitly, respectively. This holds true even if the process used can be shown that it considers the resilience engineering paradigms.

To overcome this, a joint risk and resilience analysis and management process in five steps is given by Fig. 3.

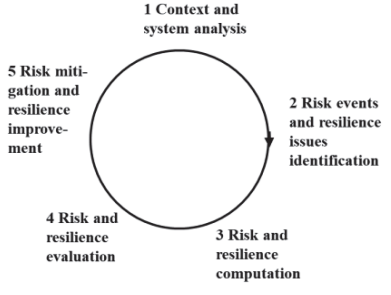

Fig. 3. Risk control and resilience analysis and improvement cycle conformal with 31000, 2018.

3. Circles for Crisis and Disruption Handling

When dealing with emergency or disruptions response phases, one should take into account the disaster risk management cycle (DRMC) consisting of preparation, response, recovery and mitigation, see e.g. for a more recent presentation (OCHA 2019).

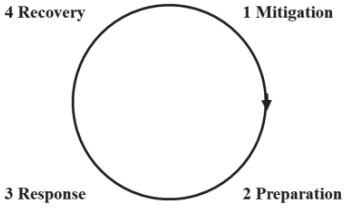

Fig. 4. Disaster risk management cycle example.

The following 5 phases are often used in the civil security research context, in particular regarding critical infrastructure protection, see (Thoma et al. 2016): 1. Prepare, 2. Prevent, 3. Protect, 4. Respond, 5. Recover, see Fig. 5.

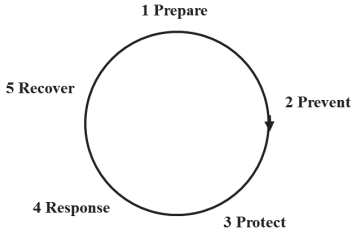

Fig. 5. Resilience cycle: Disruption management steps timeline and logic, according to (Thoma et al. 2016).

It has been argued that these steps also can be applied to engineer resilience solutions for smaller systems and solutions, see (Häring et al. 2016).

When resorting to health monitoring, surveillance and active protection also the following additional refining steps can be used:

1. Prepare (organizational, cyber, technical, physical including physical-structural; for all steps 2 to 6),
2. Detect,
3. Prevent,
4. Protect (active protection in case of events),
5. Respond,
6. Recover (to improved) system performance,
7. Learn and adapt (covers steps 2 to 6).

The steps are shown in Fig. 6. Step 1 preparation can be understood to comprise all preparatory measures as soon as new information is available, e.g. after detection. Similarly, less strongly sorted logically and with respect to time, can the seventh step be understood. Steps 1 and 7 fit nicely together as step 1 can be understood to take up and implement what has been learned in step 7.

The refined resilience circle of Fig. 6 takes up such paradigms as the resorting of Caesar's famous dictum *veni, vidi, vici* (Caesar and Guthardt (Ed.) 2003) to *vidi, veni, vici* as more explicitly e.g. expressed in the often-employed OODA loop: 1. Observe, 2. Orient, 3. Decide, 4. Act. It also takes up the increasing situation and self-awareness of systems, their increasing smartness as well as their increased range of active capabilities.

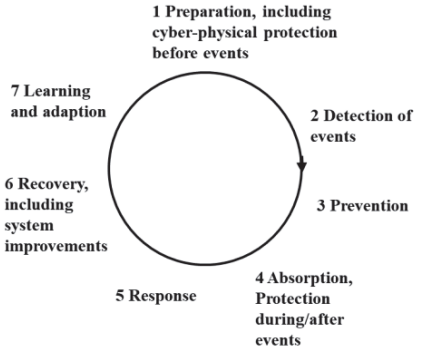

Fig. 6. Refined resilience cycle for socio-technical systems.

In terms of technologies these system capabilities are driven in particular by ubiquitous sensing, computing, reconfigurable systems, improved machine learning approaches and more flexible actuators.

4. Panarchy Processes in Socio-Environmental Sciences

When inspecting Fig. 1 to Fig. 3 and comparing with Fig. 4 to Fig. 6 similarities and overlaps can be seen. The question arises how to combine them.

Besides expanding to a big circle, an option is to use a panarchy, indicating that two qualities are considered as described in section 1. Each part of the panarchy loop can represent such qualities and how they are connected.

The most often used panarchy loop for considering (socio) ecological resilience is shown in Fig. 7 in rather standard form as used in (Allen et al. 2014).

The idea of the adaptive cycle is best explained with the life of a single tree using the standard notation. It covers the living and non-living elements of the system in its domain, its growth and decay, see (Allen et al. 2014) and the conventional notation introduced by Holling (1985):

- r phase: phase of growth,
- K phase: conservation phase,
- Ω phase: release phase,
- α phase: reorganization phase.

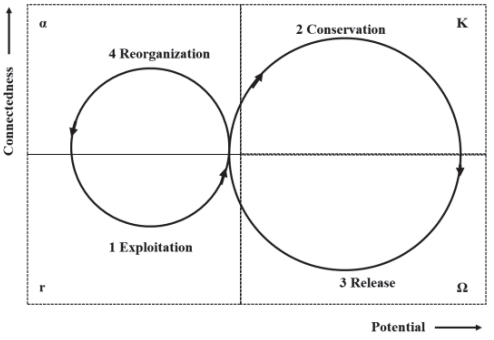

Fig. 7. Adaptive cycle or panarchy as used in ecological and socio ecological sciences according to (Allen et al. 2014).

The idea of the adaptive cycle is best explained with the life of a single tree using the standard notation. It covers the living and non-living elements of the system in its domain, its growth and decay, see (Allen et al. 2014) and the conventional notation introduced by Holling (1985):

- r phase: phase of growth,
- K phase: conservation phase,
- Ω phase: release phase,
- α phase: reorganization phase.

Within the shorter initial r phase rapid exploitation of resources takes place, e.g. the tree seed starts growing. The K phase takes longer and consists of accumulation of resources (more connected and overall more potential of the system elements when compared to the environment), e.g. the tree takes its place in the wood. Within the Ω phase the system is disintegrated or released due to not being capable to sustain, for instance not being able to adopt or due to lack of resilience to single events, e.g. less water supply or simply by aging. In the α phase the system elements are reorganized and become ready for new arrangements, e.g. the tree material becomes fertile soil.

Obviously, it is not straightforward to transfer all the domain specifics to (socio) technical systems. Nevertheless, at least the following key ideas in the phase panarchy model are potentially transferable:

- Long-term successful systems, when considered as part of a greater system, can allow for almost complete destruction if they are capable of reorganization from a seed system.
- From a true long-term perspective there is no stable system.
- The more aggregated and bigger a system becomes, the more it is vulnerable to disruptions and lack of resilience.

- The topology of the infinity loop (panarchy) allows for the expression of complex rearrangement processes.
- The panarchy loop crossing topology can be used to define a directed process. There is a transition between phase 1 and phase 2 but not between phase 1 and phase 3 as well as not between phase 1 and phase 4. This is expressed in Fig. 7 by the two arrows in the center of the figure, which are put on the only allowed transition line from the left hand side to the right hand side. The transition line between phase 3 and phase 4 is below.
- Panarchy loops can also be used to express the relative duration of phases and such properties as e.g. potential and connectedness.
- There remains a certain level of heuristics in such schemes.

The next section explores potential combination options of the joint risk and resilience analysis and management cycle and the disruption handling cycle.

5. Combination Options of Risk and Resilience Analysis Circle and Disruption Management Circle to Panarchy Process

This section considers different panarchy combination options considering Fig. 3 and Fig. 6 as starting circles. This are clockwise directed circles. So, in principle there are four options of combining them into a panarchy: The risk and resilience management cycle can be at the left hand side and the disruption handling cycle at the right hand side, or vice versa; the directions of both can be inverted. The idea is that, at least for all known threats, there is first analysis and then handling of disruptions. Hence the very first option is selected.

Next the question is addressed where to connect the cycles. This implies a transition of quality from one half of the panarchy to the other as discussed in section 4. For instance, one option is to allow for a transition between potential risks or disruption events as analyzed within the joint risk and resilience analysis and management cycle and real such occurring events, in particular as such events are detected. In this sense the panarchy crossing marks the transition from virtual analysis of events to real world events.

When inspecting the direction of the left hand side of the circle of the panarchy of Fig. 7 it has a different direction when compared to the right hand side circle. This implies that at least one of the circles of Fig. 3 or Fig. 6 has to reverse its direction. As the risk and resilience analysis and management circle has already the clockwise direction and has been decided to be the first circle of the panarchy, the direction of the crisis or disruption management cycle (resilience cycle) is reversed.

Combining the ideas of the last two text sections, when moving the two named phases opposite to each other, i.e. the risk event and disruption event identification phase of Fig. 3 and the disruption detection phase of Fig. 6, the two circles can be combined into a panarchy. Fig. 8 presents the resulting panarchy loop.

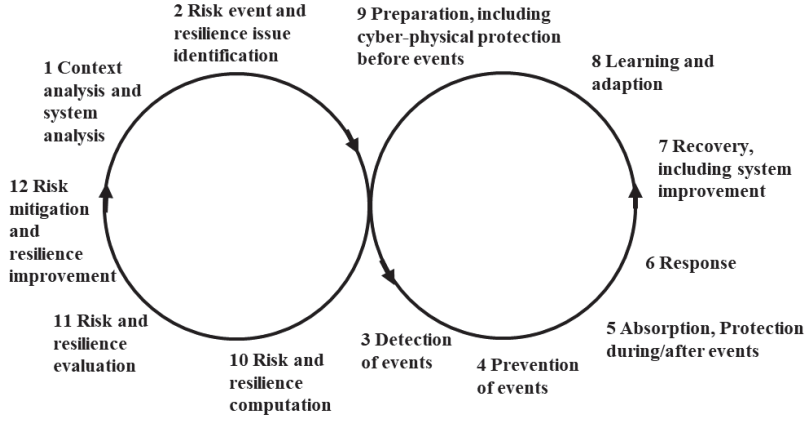

Fig. 8. Joint risk and resilience analysis, management and handling cycle with transition from analysed risks and disruption events to materialized risks and disruption events.

When inspecting Fig. 7 and Fig. 8 one finds opposite directions of the panarchy circles. This is due to the decision to put the risk and resilience analysis and management circle first and not to reverse its order. Another rather trivial observation is that each circle can be conducted stand alone: a transition from phase 2 to phase 10 as well as from phase 9 to phase 3 is meaningful

by just reproducing respectively Fig. 3 and Fig. 6, with slightly shifted order of phases. This is different from the adaptive panarchy of Fig. 7.

The transition of phase 2 to phase 3 of Fig. 8 is meaningful in the sense of that an identified potential threat or resilience issue (short term for critical combination of system performance function and threat or disruption) can materialize.

On the other hand, the transition from phase 9 to phase 10 is much less intuitive: it is not credible that a potential threat or resilience issue can only be analyzed if it already was treated in reality, i.e. is an exampled threat.

In this light, the right hand side loop of Fig. 8 could be interpreted as virtually conducting the respective steps taking into account past experiences, in addition not necessary with the same system, but any similar system. In this sense the left hand side circle could be interpreted as being conducted first for analysis purpose and second in case a threat or resilience issue materializes.

The second natural panarchy construction option is by switching from the risk mitigation measure and resilience improvement implementation phase 5 of Fig. 3 to the preparation phase 1 of Fig. 6, see Fig. 1. . In this case, before the panarchy crossing point all phases of the risk and resilience analysis and management cycle can be completed.

As expected, at transition from phase 2 to phase 10 of Fig. 1. is also feasible corresponding to the second iteration of risk analysis and management to systematically consider secondary risks. Also the right hand side of Fig. 1. can be conducted on its own, i.e. the transition between phase 12 and phase 6 is feasible and meaningful, an iteration can be understood as a second realization of a disruption or a reassessment to identify secondary effects of resilience improvement measures. Again in this case, before the panarchy crossing point all phases of the resilience cycle can be completed.

The transition between phase 5 and phase 6 of Fig. 1. is very smooth and can be understood as a stronger focus on actionable preparation, closer to the actual doing, after all risk control and resilience improvement measures deemed necessary have been implemented. The phases are so similar that they even could be merged. However, they use technical terms with strong connotations in the respective communities.

Also, the transition between phase 12 and phase 1 of Fig. 1. is rather straightforward as an adopted system that learned from past events needs to be understood again and also the context may change.

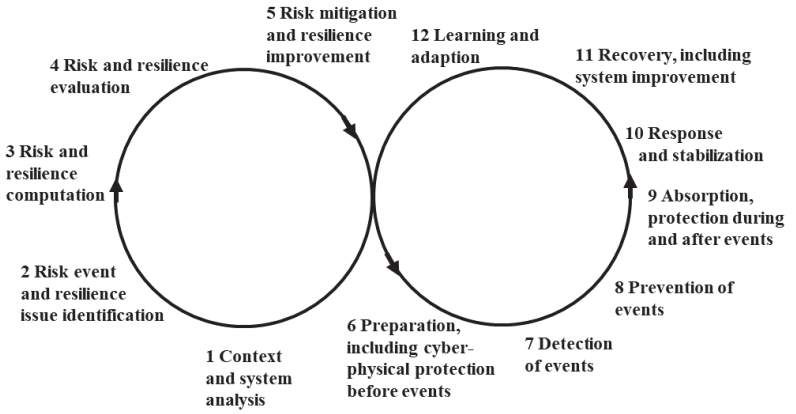

Fig. 1. Joint risk and resilience analysis, management and handling cycle with transition from risk and resilience measure implementation to preparation phase.

The second option with transition from risk mitigation and resilience enhancement to preparation (see Fig. 1.) is found more convincing when compared to the first option with transition from risk event and resilience issue identification to its detection (see Fig. 8). Both panarchies generate a joint risk and resilience assessment, risk control and resilience improvement as well as disruption event handling process, a joint risk and resilience assessment, improvement and management panarchy or system resilience panarchy process.

For the second option when compared with the first option the following statements hold:

- Each circle can be conducted completely (before moving over to the second circle).
- The steps close to the intersection are better related to each other.
- The joining idea of the circles is less conceptual.

- It has the potential to further reduce the analysis steps (however only with the drawback of being less explicit and less concept-inclusive).
- The right hand side can be better used virtually since when already phase 1 to phase 5 are conducted as opposed to the first option where only two steps are conducted.
- In both panarchies, the circles have a similar number of phases. In the second case, the resilience cycle could be reduced to five steps by combining e.g. phases 7 and 8 and phases 9 and 10, respectively.

6. Usability of Simulation Method in All Panarchy Phases for Critical Infrastructure Sample System

The section shows for the exemplary method dynamic gas grid flow simulation its potential use in all phases. Table 1 gives examples for each panarchy phase according to Fig. 1. . The sample system is the overall gas grid supply system as covered by the European research project SecureGas (2020).

Gas grid simulation refers to real gas flow simulations in case of standard and leaking gas pipelines as for instance described in (Kostowski and Skorek 2012), which allows to determine the time dependent local pressures, flows and temperatures of natural gas within pipelines. Such approaches go beyond topological graphical gas grid simulations as e.g. described in (Praks et al. 2015), which use for instance the maximum flow approximation. They can be used to improve graphical simulations. However, are still too slow for comprehensive resilience quantification.

Table 1. Usability of gas dynamic flow simulation method in panarchy phases for gas grid critical infrastructure on European scale.

Risk control and resilience analysis, improvement and management panarchy phase	**Use of simulation in phase**
1 Context and (performance function) system analysis	Define which (time-dependent or integral) quantities should be determined by simulation approach (verbose and formal description)
2 Risk event and resilience issue identification	Determine which threats and disruptions should be simulated (e.g. local, short term or long term) and how to model them
3 Risk and resilience computation	Conduct the simulation in the analysis phase to determine the effects of threats and disruptions using the risk control and resilience quantities for single events and overall
4 Risk and resilience evaluation	Ensure that the computed quantities can be communicated and compared with risk criteria and other acceptance criteria
5 Risk mitigation and resilience improvement	Compute the effects of risk mitigation and resilience improvement options
6 Preparation, including cyber physical protection before events	Compute the effects of the preparation measures
7 Detection of events	Determine by simulation signs of events and resilience issues, e.g. loss of pressure in case of leakage, or oscillations caused by external inference
8 Prevention of events	Compute options of preventing significant effects of events, e.g. by increasing or decreasing gas compression, or by adding redundancies
9 Absorption, protection during and after events	Determine the absorption capacity and the efficiency of physical reactive measures, e.g. of the effect of gas storage and coordinated steering of valves
10 Response and stabilization	Determine the effects of disruptions, e.g. till stabilization of scenarios
11 Recovery, including system improvement	Compute how the system recovers, e.g. according to repair strategy of leakage of pipelines or redirection of gas flows
12 Learning and adoption	Compute the effects of modified system designs within systematic system optimization approaches

7. Conclusions

The paper set out to combine the five step risk analysis management cycle and the resilience cycle inspired from the four step catastrophe management cycle within a meaningful panarchy process. It found that when starting out with the former, there is a kind of natural way of connecting the two processes, when resorting to current versions of the circles.

It was found that the resulting joint risk control and resilience assessment, improvement and management panarchy has a different topology when compared to the adaptive panarchy, which is often used in the socio and environmental sciences. This holds because of the meaningful looping within each circle of the proposed system resilience panarchy process, the option of virtual looping to consider what-if scenario handling by going through the right circle of the panarchy (see Fig. 1.) and because of the need for iterations till convergence to consider higher order effects due

to risk control and resilience improvement activities.

The steps of the proposed resilience panarchy were motivated resorting to the respective two circular original processes. Hence, they are believed to be well defined and distinguishable. This was illustrated for the sample method predictive physical engineering gas flow simulation and its application to natural gas supply grids by showing which activities are expected to be conducted in the resilience panarchy phases.

Further work could explore the application of the system risk control and resilience panarchy process to a selected critical infrastructure. This could be conducted by identifying a complete set of methods and giving an overview of their results with focus on coverage and rigor of findings. Another approach could be to provide detailed simulation results and discussing them supported by the panarchy process and panarchy phase objectives for given infrastructure (sub) systems.

Acknowledgements

The work has in parts been supported by the EU project SecureGas (Grant No. 833017) on cyber-physical security of gas grid critical infrastructure.

References

31000 (2018) Risk management - Guidelines. ISO 31000, Geneva, Switzerland

Allen CR, Angeler DG, Garmestani AS, Gunderson LH, Holling CS (2014) Panarchy: Theory and Application. Ecosystems 17:578–589.

Aven T (2019) The call for a shift from risk to resilience. What does it mean? Risk Analysis 39:1196-1203.

Caesar GI, Guthardt (Ed.) A (2003) Bellum Gallicum

Fehling-Kaschek M, Faist K, Miller N, Finger J, Häring I, Carli M, Battisti F, Makri R, Celozzi G, Belesioti M, Sfakianakis E (2019) A systematic tabular approach for risk and resilience assessment and improvement in the telecommunication industry. In: Beer M, Zio E (eds) Proceedings ESREL 2019. pp 1312–1319

Häring I, Ebenhöch S, Stolz A (2016) Quantifying Resilience for Resilience Engineering of Socio Technical Systems. European Journal for Security Research 1:21–58.

Häring I, Sansavini G, Bellini E, Martyn N, Kovalenko T, Kitsak M, Vogelbacher G, Ross K, Bergerhausen U, Barker K, Linkov I (2017) Towards a generic resilience management, quantification and development process. In: Linkov I, Palma-Oliveira JM (eds) Resilience and risk: Methods and application in environment, cyber and social domains. Springer, Dordrecht, pp 21–80

Holling C (1985) Resilience of ecosystems: local surprise and global change. In: Malone TF (ed) Global change: The proceedings of a symposium sponsored by the Internat. Council of Scientific Unions (ICSU) during its 20. general assembly in Ottawa, Canada on Sept. 25, 1984. Cambridge Univ. Pr, Cambridge, pp 228–269

Hollnagel E, Woods DD, Leveson N (eds) (2006) Resilience engineering: Concepts and precepts, transferred to digital printing. Ashgate, Farnham

IEC 61508 (2010) Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508

Kostowski WJ, Skorek J (2012) Real gas flow simulation in damaged distribution pipelines. Energy 45:481–488.

Lalonde C, Boiral O (2012) Managing risks through ISO 31000: A critical analysis. Risk Manag 14:272–300.

Olechowski A, Oehmen J, Seering W, Ben-Daya M (2016) The professionalization of risk management: What role can the ISO 31000 risk management principles play? International Journal of Project Management 34:1568–1578.

Praks P, Kopustinskas V, Masera M (2015) Probabilistic modelling of security of supply in gas networks and evaluation of new infrastructure. Reliability Engineering & System Safety 144:254–264.

SecureGas (2020) Securing the European gas network: EC Grant agreement ID: 833017.

Thekdi S, Aven T (2019) An integrated perspective for balancing performance and risk. Reliability Engineering and System Safety 190:106525.

Thoma K, Scharte B, Hiller D, Leismann T (2016) Resilience Engineering as Part of Security Research, Eur J Secur Res 1:3–19.