Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

The Kursk submarine disaster in view of resilience assessment

A. Leksin & U. Barth
University of Wuppertal, Wuppertal, Germany

R. Mock
Zurich University of Applied Sciences, Winterthur, Switzerland

ABSTRACT: In August 12, 2000, the Russian Oscar-class submarine Kursk (K-141) sank during a navy manoeuvre in the Barents Sea killing all 118 personnel on board. The vessel was powered by two nuclear reactors and carry nuclear missiles which can be armed. The disaster is well documented and encompasses many socio-technical elements influencing the sequence of events finally leading to wreckage. For this, the disaster is considered as an archetypical event which might highlight the advantages as well as the limitations of resilience assessment approaches, e.g. in comparison with established risk assessment methodology. For this the paper starts with results of a literature survey with resilience metrics and areas of technical applications. The Kursk disaster is reviewed by available literature and research reports by Root Cause Analysis. The causing aspects (events, procedures, human factors, etc.) are then structured and classified according to their relevance and impact on vessel's resilience. In a next step, these aspects are contrasted to the risk assessment approach as defined, e.g. by ISO 31000. The methodological juxtaposition is intended to characterize the maturity level of resilience analysis in a real world framework as well as to elaborate major differences in validity of the underlying system analysis concepts. Finally, the pros and cons of the reviewing approach are discussed.

1 INTRODUCTION

In the context of risk analysis, the term resilience is often used nowadays. It is noticeable that both a generally accepted definition of this term and consequently a metric of resilience are missing. The differences between risk and resilience assessment often remain unclear, e. g. in connection with related terms such as availability, vulnerability, and Business Continuity Management (BCM). To a certain extent, this follows a tradition of dealing with indefinite terms such as, risk, which in turn is based on other terms that are not always clearly definable. For instance, there is a risk if several factors coincide: danger, exposure and vulnerability (cf. (Lenz 2009)).

The paper is an attempt to work out the differences and similarities between the two concepts of risk and resilience, where the approach follows the idea of "learning by doing" system assessments. An archetypical case was selected for this: The Kursk submarine disaster in 2000. On the one hand, a submarine is a self-contained socio-technical system, which simplifies considerations. The case itself, in turn, can be presented from a variety of sources. One of us (A. Leksin) can refer to less well known Russian literature as well as on feedback of one Russian accident investigator. The case was dealt with a root cause analysis (RCA), which was then used for the discussion on risk and resilience assessment.

The remaining paper is structured as follows: Chapter 2 compiles definitions of risk, resilience and the comparison of major system management terms. Chapter 3 describes the chronology of major events and causative aspects of the Kursk disaster and present a part of the resilience identification. Based on sequence of major events differences in risk and resilience assessment are elaborated in chapter 4. The results are discussed in chapter 5.

2 TERMINOLOGY

There is extensive literature research on the definition of the term resilience, e. g. (Husseini et. al. 2016, Francis et al. 2014). There is a consensus that resilience is concerned with socio-technical systems and their ability to respond to disturbances in order to maintain the specified performance. This paper follows the definition of (Lay et al. 2015) who defines resilience by a set of system abilities:

Resilience: System abilities to respond to disturbances, to monitor, to learn, and to anticipate developments.

Table 1. Comparison of major system management terms.

Term	Connotation	Intrinsic system property	Management	Focus
Risk	negative	no	external interference	(undesired) events
Resilience	positive	yes	Intrinsic	System performance
Vulnerability	negative	yes	external interference	(undesired) flaws
BCM	positive	no	external interference	(undesired) events
Availability	positive	yes	external interference	failures

Responsiveness considers all kind of disturbances into account, all deviations from specified performance levels, both positive and negative impacts. The term "disturbance" indicates that point of view is dominated by negative impacts.

Furthermore, responsiveness indicates systems immediate response to disturbances. Hence resilient systems are designed to react on disturbances in a self-managing way.

Looking at socio-technical system, humans are the carrier of its learning and anticipating abilities as covered by system management processes. Monitoring can be done both automatically/technically and by humans also depending on surveillance level.

The concept of risk is assumed to be known to the reader. The paper follows the well-established definition of risk of (Kaplan & Garrick 1981):

$\{\mathrm{Risk}_i \mid s_i,f_i,c_i\}$,
where:
S_i: scenario identification or description
F_i: probability (or frequency) of that scenario
C_i: consequence or evaluation measure of that scenario, i.e., the measure of damage.

The frequency/consequence concept of risk is also along to common risk management standards, e.g. (ISO 31000 2009). Risk figures are usually computed by $f_i \cdot c_i$. Note, that scenario is not defined by (Kaplan & Garrick 1981) and (ISO 31000 2009). The authors will use it in terms of (imagined) sequence of events. Probability is a measurement of uncertainty of (future) events based on (statistical) data. As a consequence, risk becomes a concept of proactivity and finally preparatory by management.

Vulnerability is a well established term in IT security which is easily adaptable to any other engineered systems. According to (NIST 2012), the definition is:

Vulnerability: Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.

For this, the understanding of vulnerability follows the keyhole principle and is an intrinsic system property. Vulnerability management is then to reactively plug flaws.

However, the limits of the concepts are not always clear: According to (Lenz 2009:38–43.69), risk always coincides with danger, exposure and vulnerability. Additional components such as coping capacity and criticality (meaning and consequences upon entry) can be added to this assumption.

The concept of Business Continuity Management is a related system maintaining process to risk, resilience and vulnerability management, as defined by (SBA 2013):

Business Continuity Management (BCM) is a company-wide approach designed to ensure that critical business processes can be maintained in the event of major internal or external incidents.

The view is the management of single (major) undesired events in order to minimise their impacts. The management objective is to maintain the specified business performance level.

3 THE SUBMARINE KURSK (K-141) DISASTER

The Kursk submarine disaster took place in the Barents Sea on 12 August 2000, killing all 118 personnel on board. In this paper, the course of the disaster, if publicly known, serves as a test case for the methods of system analysis listed in chapter 1. The detailed description of the disaster is a significant part of the resilience identification step which is explained in chapter 4.2. The authors process the Kursk catastrophe on the basis of publicly available information and present a possible sequence of events. Further discussions will then be held on this basis. The case covers all elements that make an analysis interesting from very different perspectives, i.e. the interaction of people and technology in a stressful overall situation. However, the basic system performance remains simple: *ensuring the safety and health of the crew*. The question is to what extent the system analysis methods listed above would have been suitable for recognizing this accident in advance.

3.1 *Event of the Kursk disaster*

There are about 18 different disaster versions of the Russian Oscar-class submarine Kursk (K-141).

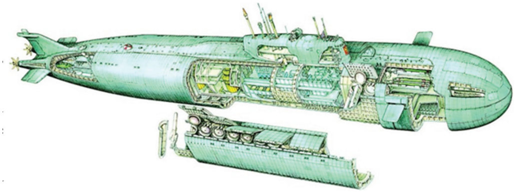

Figure 1. Example of the inner and outer hull construction with P-700 Granit “Shipwreck” cruise missiles on the bow side (Militaryarms 2017).

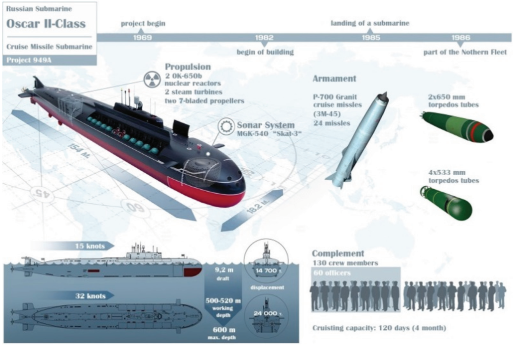

Figure 2. Characteristics of Oscar class submarine (Defending 2015).

This paper considers one of the official versions—an explosion of a torpedo but due to the influence of a second submarine. The chronology of major events and causative aspects (events, procedures, human factors, etc.) are structured and classified according to their relevance to give a better overview for the reader by describing only the important steps of the disaster. The RCA breaks down a complex scenario into individual steps (black boxes in the RCA diagram of Figure 3), which ultimately indicate a cause-effect chain. Secondary event chains can be added (grey boxes). For better understanding the boxes are numbered. The event numbers can also be found in the case description.

Table 2. Explosive characteristics of USET-80 and VA-111.

USET-80 (warshot torpedo)	Total weight – 2000 kg explosive weight – 200/300 kg
VA-111 (warshot torpedo)	Total weight – 2700 kg combat unit – 200 kg explosive weight 200 kg

The description of the significant factors which had a strong influence on the worst case scenario can be traced back to 1999. Kursk was on the military mission in the Mediterranean Sea to monitor the United States Sixth Fleet responding to the Kosovo crisis. *(1)* After the successful mission the submarine returns into the stationing port of Vidyayevo. After a longer down time due to financial reason the commissioning of the submarine by the crew was under time pressure towards the end of May 2000 because of the Russian Navy large scale naval exercise planning for August 2000. Therefore the crew had a shortage of lack of planned training activities in the last approx. 9 months *(2)*. But due to the last successful mission in the Mediterranean Sea, it cannot be ruled out that part of the crew was self-confident. Either because of time pressure and/or the incorrect planning of the Marine areas by the Military-Maritime Fleet of the Russian Federation *(3)*, the way to the naval exercise area was over “underwater mountains” *(4)*. Such manoeuvre through areas of not deep-water sites of the sea can be dangerous for an Oscar-class submarine and other submarines because it is difficult to manoeuvre due to radar shadows of sonar and magnetic interference. The threat obviously increases with the condition that other countries submarines are always present in such naval exercises.

On August 10th, 2000 the Kursk had begun the planned activities in the naval exercise near the Kola Bay. On August 12th, 2000 at 11:28 local time, two explosions were detected by various seismologists and hydroacoustics. The first explosion corresponded for ≈500 [kg] TNT equivalent and after 135 seconds the second explosion with ≈5000 [kg] TNT equivalent. Unfortunately the exact number of armed cruise missiles at the Kursk varied depending on references. Typical armament consist 24 of SS-N-19/P-700 Granit “Shipwreck” cruise missiles that were designed to defeat the best naval air defences. The missile containers are located on both sides of the deckhouse, outside the rugged boat hull. Based on the most references, photographic material and video footage the Kursk had during this naval exercise 24 of P-700 Granit “Shipwreck” cruise missiles on board. Due to the double hull construction of the Oscar-class submarine, the second explosion of the P-700 Granit “Shipwreck” cruise missiles did not initiated. Constructors considered such worst-case scenario and reinforced the inner hull with high content stainless steel about 45–68 [mm] thick. There is 200–350 [cm] gap to the 5–10 [mm] thick outer hull.

Therefore both detected explosions were in the 1st torpedo compartment. As before the exact number of dummy and warshot torpedos varies from 8 to 18 and even 24. Weapons included 18 of SS-N-16 “Stallion” (РПК-6 “Водопад”), hydrogen peroxide-fueled Type 65 torpedo (65–76A), USET-80 (УСЭТ-80) and their different types. Kursk was armed at that moment with dummy (65–76ПВ and USET-80) and warshot (65–76A, USET-80) as well as torpedo VA-111 Shkval.

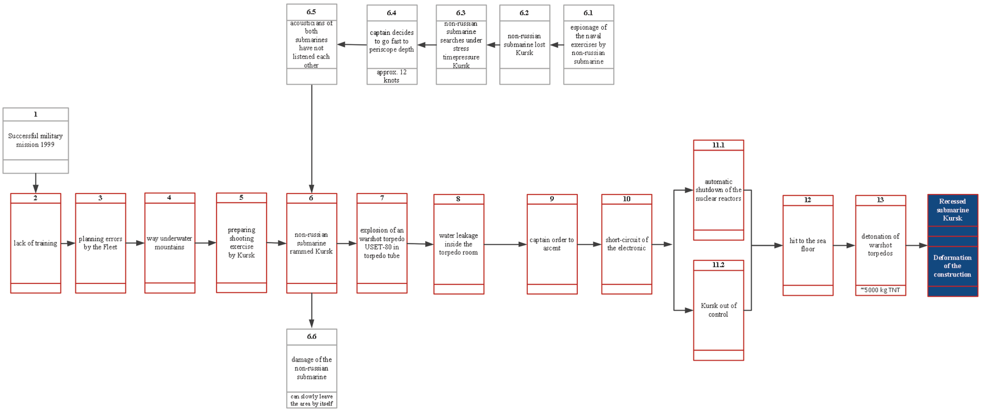
6.5
acousticians of both submarines have not listened each other
6.4
captain decides to go fast to periscope depth
approx. 12 knots
6.3
non-russian submarine searches under stress timepressure Kursk
6.2
non-russian submarine lost Kursk
6.1
espionage of the naval exercises by non-russian submarine
1
Successful military mission 1999
2
lack of training
3
planning errors by the Fleet
4
way underwater mountains
5
preparing shooting exercise by Kursk
6
non-russian submarine rammed Kursk
7
explosion of an warshot torpedo USET-80 in torpedo tube
8
water leakage inside the torpedo room
9
captain order to ascent
10
short-circuit of the electronic
11.1
automatic shutdown of the nuclear reactors
11.2
Kursk out of control
12
hit to the sea floor
13
detonation of warshot torpedos
~5000 kg TNT
Recessed submarine Kursk
Deformation of the construction
6.6
damage of the non-russian submarine
can slowly leave the area by itself

Figure 3. Sequence of events in form of RCA.

Although it was an exercise, Kursk loaded, as mentioned before, also with combat capable weapons. This means that some of the torpedo tubes are constantly in combat readiness with an armed warshot torpedo. Warshot torpedo which was used by Kursk in military mission is typically the torpedo USET-80. Table (2) shows short characteristics of the torpedoes USET-80 and VA-111 Shkval.

Based on these characteristics, the possibility of an USET-80 in the torpedo tube is very high and its TNT equivalent is near to 500 [kg] *(7)*. Also it was planned to launch the USET-80 torpedo as secondary in this naval exercise.

However, all versions of disaster reports agree on one—the first explosion was an explosion of a torpedo in a torpedo tube. As mentioned before, by all naval exercises other countries submarines are always present at the naval area as well as near main marine ports during the year. The history of underwater incidents between submarines is well known and documented in different languages and countries (Drew et al. 1998). “Among the specified accidents there are several tens of collisions of submarines, including 20 underwater collisions of Russian Navy submarines with foreign submarines. From these 20 examples 11 were in grounds of combat trainings (naval exercises) on the way to the main stationing sites of the Northern and Pacific fleet, including 8 in the north and 3 in the Pacific Ocean in a short time period from 1968 till 1993” (Aleksin 2001, Viperson 2001). Several accidents have also been registered since 1993 till nowadays. On August 12th, 2000 Kursk prepares for shooting practice in the predetermined and surveyed area radio and radio engineering investigation of surface forces of “opponent—Kirov-class battlecruiser Pyotr Velikiy” *(5)*. Due to force 3 at sea the speed of Kursk was approx. 8 knots. The Kursk had changes the depth level many times according to typical exercise. A second non-Russian submarine which monitors Kursk the last two days *(6.1)* has lost the contact *(6.2)* and couldn’t find the Russian submarine *(6.3)*. They decided to emerge on periscopic depth *(6.4)* to explain this situation in order to prove if Kursk has also surfaced. On the way to periscopic depth the non-Russian submarine unexpected struck *(6.5)* with the lower cornice of a bow part from a high angle of attack to the top area of the right bow side of Kursk where were torpedo tube was charged with the warshot torpedo USET-80. Both submarines continue to move with a former speed (5.5 [m/s]), destroying each other’s hulls *(6)*. Nuclear submarines of US and UK Navy are build only one 35–45 [mm] thick stainless steel hull. Thus Kursk damage was much higher. In a second after the struck with the torpedo tube located to the right board of Kursk it was crumpled on a half of the length which caused a detonation of the warshot torpedo USET-80 *(7)*. This detonation was on a line of least resistance to the hatch of the torpedo tube, destroying this and created a hole more as half a meter in diameter. Water flows inside the torpedo compartment and causes trim to the bow side *(8)*. The captain of Kursk order to ascent and increase the speed *(9)*. However short circuits of electrical networks happen because of water penetration *(10)* and due to this the emergency system block both nuclear reactors *(11.1)*. The Kursk was out of control *(11.2)* with a strong trim to the bow side and hits the seafloor *(12)*. The second explosion was initiating with the impact on the floor *(13)*. This explosion killed many crew members in the conning tower and control room (2 compartment), radioelectronics room (3 compartment), living room (4 compartment), room with diesel-generator, electrolysis installation for air regeneration, compressors of high pressure etc. (5 compartment). Although Kursk was designed to withstand external pressure of depths of up to 1.000 [m], the second internal explosion destroyed the bulkheads between the compartments (probably till the compartment 5) which are calculated for only 10 atmospheres.

The inner hull is designed for 60 atmospheres, which prevented the explosion of the P-700 Granit "Shipwreck" cruise missiles as mentioned before in this paper.

Based on the RCA and literature statistics on similar incidents, the catastrophe must be considered by the submarine Kursk as an archetypal event. Next chapter discusses how such scenario could be implemented in the prospective of classical risk analysis as well as the possible approach of a resilience concept and its implementation problems.

4 RISK AND RESILIENCE ASSESSMENT

The established system assessment process can be summarized by three steps: *identification, analysis, evaluation*. These processes are well defined in risk assessment while there are methodological gaps in resilience assessment.

The following subsections outline these gaps and point to differences in risk and resilience assessment by exemplary application to the Kursk disaster.

4.1 *Risk assessment*

The established approaches and concepts of risk assessment are presumably known to the reader (i.e., how to perform Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), and others).

Also in risk assessment, a study starts with determination of system boundaries. When following the risk management process of, e.g., ISO 31000, then risk assessment includes the (technical) system, where the remaining risk managing processes are beyond. With regard to resilience assessment (cf. chapter 4.2), risk studies are based on a restricted system definition. As a consequence, some boxes of RCA in Figure 3 are excluded (the results of all selection criteria as compiled in this chapter are applied on RCA of the Kursk disaster and summarized in Table 3).

There are studies of navy available to support out established risk assessment approaches, e.g., (Holmboe et al. 1992) on likelihoods of threats, maturity of technologies, systems potential to develop a threat scenario.

The identification process starts with the specification of hazards and threats as well as vulnerabilities of the system and system components.

Hazard is commonly defined as a condition, circumstance or process what can cause damage. Furthermore, hazard is limited to accidental, undesired and sudden events.

Risk analysis needs the quantification of frequency and likelihood of an undesired event. Figure 5 shows the risk analysis model as applied by the authors.

The terms in Figure 5 are specified by:

- hazards are characterised by possibilities,
- results of threat factors. Scenario analysis used to anticipate how threats and opportunities might develop and are used for all types of risk with short and long term time frames,

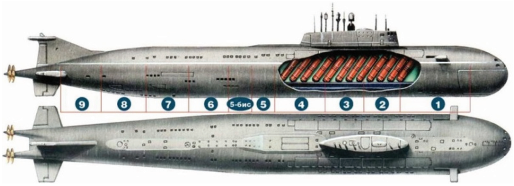

Figure 4. Compartments of Kursk (Naked-science 2017).

Table 3. Risk analysis relevant actions according to RCA.

RCA steps	Action	*H*	*T*	*V*	*S&S*	*C*
2	negative	+	–	+	n.r.	–
3	negative	+	–	+	n.r.	–
4	negative	+	+	–	n.r.	+
5	n.r.	n.r.	n.r.	n.r.	n.r.	n.r.
6	negative	+	+	+	+	+
7	negative	+	+	+	+	+
8	negative	+	+	+	+	+
9	n.r.	n.r.	n.r.	n.r.	n.r.	n.r.
10	negative	+	–	+	+	+
11.1	positive	n.r.	n.r.	n.r.	n.r.	+
11.2	negative	+	–	–	–	+
12	negative	+	+	–	+	+
13	negative	+	+	+	+	+
End	negative	+	+	+	+	+

+: relevant impact regarding risk analysis; –: no-impact on defined system; n.r.: not relevant for risk analysis.

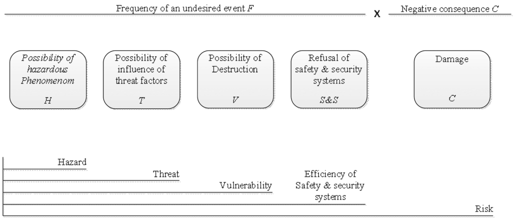
Frequency of an undesired event *F*
x
Negative consequence *C*
Possibility of hazardous Phenomenom
H
Possibility of influence of threat factors
T
Possibility of Destruction
V
Refusal of safety & security systems
S&S
Damage
C
Hazard
Threat
Vulnerability
Efficiency of Safety & security systems
Risk

Figure 5. Risk analysis model.

- destruction of objects as a result of hazards are characterized by conditional probability,
- unavailability of safety and security systems because of combinations of non-reliability, human factors among others, are quantified by probabilities of scenario development from emergencies towards accident.

Depending on analysis goals (quantitative or qualitative) different approaches are in use. The Russian Army carries out FTA (personal communications with Saint Petersburg State Institute of Technology). However, FTA does not consider positive events and an analysis of top event *Recessed submarine* is then incomplete. The failure analysis based on qualitative approaches, as FMEA, could be added.

Within this defined framework for risk analysis Table 3 shows the relevant boxes of the RCA.

The selection process for identifying the RCA boxes relevant to risk analysis bases on the following rules:

Rule 1: The box event is within the defined system boundary.
Rule 2: The hazard is relevant within the defined system boundary.
Rule 3: If a threat (from outside) exists, it is taken into account.
Rule 4: Searching for vulnerabilities in the system.
Rule 5: Investigation of safety and security systems is a special task of risk analysis.
Rule 6: Negative consequences are always relevant for risk analysis independent from threats and vulnerabilities.

Thus, step *preparing shooting exercise (5)* is not relevant from the view of risk assessment. The *order by the captain (9)* is a positive measure and, thus not relevant for the defined scenario. The *automatic shutdown of the nuclear reactor (11.1)* is not part of the risk analysis because it is a planned safety process. Steps *(2)* and *(3)* are only considered in human reliability analysis. Finally risk is often evaluated by risk matrix. However, the risk evaluation process is not subject of this paper.

4.2 *Resilience assessment*

As mentioned in chapter 2, resilience considers extended socio-technical systems where (human as well as automated) actors are responsible for actions to positively or negatively affect system responsive-ness. Applied resilience assessment by case study brings further differences to risk assessment in understanding to light. The system assessment processes (i.e. aspect identification, analysis and evaluation) structures the following discussion.

System performance is a matter of documented system design specifications and other characteristics of embedding system entities. Then, resilience assessment of the Kursk disaster comprises all involved submarines and crews as well as the entire Northern Military-Maritime Fleet of the Russian Federation at the moment of the exercise and impacts from sea environment. The impact on the environment is not relevant. Hence, you can easily define actions, actors, and system boundaries in Kursk example in contrast to, e.g., infrastructures. Within this framework, the identification process starts with the specification of system performance *P*. For this, two approaches are common in resilience assessment (cf., e.g., Mock 2018): either the analysts decide to model time-depending performance $P(t)$ or they compile a set of *n* resilience impacting aspects $P = \{a_1;\ a_2;\ \ldots;a_n\}$. $P(t)$ can be easily defined (e.g. safe and secure transport of crew and cargo during mission time) but finding a corresponding measurement is not always as straightforward as, e.g. oxygen content of the breathing air during mission time. Note, that availability, as shown in Table 1, is a performance model $P(t)$ showing the probability course of operability of a system. Maintenance and repair are considered as activities to keep the system resilient, and are actions of responsiveness.

The identification process by compilation of a set of aspects influencing resilience appears plain, e.g. the number of redundancies of life supports systems, educational level of crew, repair, etc. However, time dependency and the representation of systemic relationships are lost then.

The resilience analysis process by $P(t)$ follows the common processes of formal mathematical/physical of system modelling and simulation and will not be discussed here. However, the RCA presentation of the Kursk disaster in Figure 3, which follows a timeline of succeeding events, is considered as a simple representor of $P(t)$ after revision towards resilience (see Table 4). $P(t)$ analysis needs the specification of normal operation bandwidths of total system performance. For instance, the oxygen content on a submarine can be above or below a lethal threshold. The life support system may be able to provide a breathable atmosphere again, but this can be too late for the crew. In terms of resilience analysis, the responsiveness of the entire submarine system is lost as safe transport has ended. These points to specific views in resilience analysis: Total loss of performance or functionality (worst case) is excluded from analysis ("If dead you are not resilient any longer"). The analysis of impacting aspects $\underline{P}$ needs the definition of a resilience metric which is still under discussion in academia. Table 4 summarises the findings in resilience identification and analysis by the Kursk example as represented in Figure 3.

Table 4. Resilience assessment for performance "safe and secure transport of Kursk crew and cargo during mission time".

RCA	Sub-system	P	Action	Actor(s)
1	fleet	+	success	Kursk crew, fleet
2	Kursk	–		Kursk crew
3	fleet	–	preparedness	Kursk crew, fleet
4	environment	–		
5	Kursk	+	exercise	Kursk crew
6	Kurs, other sub.	–	ram	Both crews
7	Kursk	–	explosion	
8	Kursk	–	leakage	
9	Kursk	+	order	Kursk's captain
10	Kursk	n.r	short-circuit, loss of control	
11.1	Kursk	n.r	shutdown reactor	
11.2	Kursk	n.r	loss of control	
12	Kursk, environment	n.r	grounding, loss of control	
13	Kursk	n.r	detonation, loss of control	
End	Kursk	n.r		

+/–: positive/negative impact on resilience; n.r.: not relevant for resilience assessment purposes.

Table 5. Juxtaposition of risk and resilience assessment.

RCA events	Risk assessment	Resilience assessment
1	*N*	*Y*
2	*N*	*Y*
3	*N*	*Y*
4	*Y*	*Y*
5	*N*	*?*
6	*Y*	*Y*
6.1	*N*	*Y*
6.2	*N*	*Y*
6.3	*Y*	*Y*
6.4	*?*	*Y*
6.5	*?*	*Y*
7	*Y*	*Y*
8	*Y*	*Y*
9	*N*/*Y*	*Y*
10	*Y*	*N*
11.1	*Y*	*N*
11.2	*Y*	*N*
12	*Y*	*N*
13	*Y*	*N*
Summary	Y: 10 of 19	Y: 13 of 19

As figured out in Table 2, resilience assessment ends with the loss of control of the Kursk ("If faint, then you are no longer resilient"). Step *(6)* can be similarly analysed by considering RCA steps *(6.1)* to *(6.6)* which introduces the second submarine into analysis. The marine environment (step *(4)*) has been identified as challenging for submarines which does not support safe transport.

Resilience evaluation is the process of assessment. Again, the analyst depends on how resilience analysis been performed. In case of modelling $P(t)$ a characteristic value needs to be defined, e.g. the ratio of resilient operation mode to total mission time. This is equivalent, e.g. to reliability and availability analysis. The evaluation of the set of impacts P needs the definition of a resilience metric comparable to risk prioritisation value RPV in risk analysis and provided by FMEA. Evaluation criteria of acceptance/non-acceptance of resilience analysis results still needs to be defined (a resilience priority value is introduced in (Mock 2018)).

4.3 *Synopsis*

Based on RCA every single step is discussed from the side of resilience assessment in comparison to the risk assessment. Table 5 differs between the selections of *yes (Y)*, *no (N)*.

Avoidance of worst case scenario or disaster is the aim of a risk assessment. Therefore, positive or neutral (from the view of risk analysis) steps such *(1)*, *(3)*, *(5)*, *(6.1)*, *(6.2)* are not considered. But e.g. step *(9)* could be considered if the order of the captain is incorrect. Step *(2)* can be also considered only in case of human reliability analysis. Equivalent to a worst case scenario "meltdown of nuclear reactor", step *(13)* must be take into account by this disaster. Similar, step *(6)* could correspond to a "plane crash on nuclear power plant" scenario (external event). Step *(5)* is not a malfunction or optimization, but an important point in the overall process. Due to the defined performance indicator step *(6.2)* must be considered too (the second submarine is part of the whole system). As mentioned before, with defined performance indicator—safe implementation of the naval exercise for the crew—the resilience analysis ends with the step *(10)*. As mentioned in chapter 2, risk assessment often uses the basic frequency/consequence definition to get calculation values. However, the next step after description of the RCA from the side of resilience analysis is complicated due to absence of any useful values and equations which could be support the calculations and as a result the evaluation of the defined system and performance indicator.

5 CONCLUSIONS

Resilience assessment should be different from risk assessment and other related concepts and approaches. For instance, risk assessment is basically restricted to undesired events and does not cover the extended view of technical systems. On the other hand, event identification highly depends on the definition of system performance indicating resilience as a measurement of system quality.

The issue of applied resilience assessment is shown by considering the archetypical case of Kursk submarine disaster. The detailed description of sequence of steps by Root Cause Analysis shows that a precious accident analysis is significant for identification of aspects which have impacts on resilience. The specification of system performance and the view of extended socio-technical systems increase resource requirements (time, expertise, etc.) of auditing. This way of thinking definitely uncovers additional elements of system disturbances.

However, resilience analysis is still in its beginnings and there is no commonly accepted methodology and metric. In summary, resilience assessment is different to risk assessment in some ways and shows promising aspects in extended system analysis. However, further steps towards operationalisation of the resilience concept are needed.

REFERENCES

Aleksin, W. (2001). Версия контр-адмирала Алексина: “Курск” уничтожила иностранная подлодка. https://i-korotchenko.livejournal.com/1136736.html?page = 1#comments.

Defending (2015). Подводные лодки проекта 949А «Антей» https://defendingrussia.ru/enc/apl_kr/podvodnyje_lodki_projekta_949a_antej-1949/.

Drew, C., S. Sontag & A.L. Drew (1998). Blind Man's Bluff: The Untold Story Of American Submarine Espionage. ISBN 1-891620-08-8.

Francis, R. & B. Bekera (2014). “A metric and frameworks for resilience analysis of engineered and infrastructure systems,” *Reliability Engineering & System Safety*, vol. 121, pp. 90–103.

Holmboe E. & S. Seymour (1992). APL`S Submarine security program. *Johns Hopkins APL Technical Digest*, vol. 13, number 1.

Hosseini, S., K. Barker & J. E. Ramirez-Marquez (2016). A review of definitions and measures of system resilience, *Reliability Engineering & System Safety*, vol. 145, pp. 47–61.

ISO 31000 (2009). “Risk Management – Principles and Guidelines (Iso 31000:2009).” Geneva International Organization for Standardization (ISO).

Jean-Michel Carré (2004). *Video footage*: Kursk: A Submarine in Troubled Waters (French: Le Koursk, un sous-marin en eaux troubles). https://www.canal-u.tv/video/cerimes/koursk_un_sous_marin_en_eaux_troubles.13454.

Kaplan, S., & B. J. Garrick (1981). On the Quantitative Definition of Risk. *Risk Analysis 1, no. No. 1* (1981): 11–27.

Lay, E., M. Branlat & Z. Woods (2015). A practitioner’s experiences operationalizing Resilience Engineering, *Reliability Engineering and System Safety*, pp. 63–73.

Lenz, S. (2009). Vulnerabilität Kritischer Infrastrukturen, Forschung im Bevölkerungsschutz, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn 2009.

Militaryarms 2017. Подводные лодки проекта 949А «Антей»: история создания, описание и характеристики. https://militaryarms.ru/voennaya-texnika/podvodnye lodki/949a-antej/. http://militaryrussia.ru/blog/topic-398.html.

Mock, R. (2018). A quantitative approach for applied resilience assessment audits. In Proc. of European Safety and Reliability Conference (ESREL 2018).

Mock, R. & C. Zipper (2017). Risiko: Das Ende Eines Konzeptes? Sicherheitsforum (2017): 3.

Mock, R. & C. Zipper (2017). Embedding resilience assessment into risk management. In Proc. of of European Safety and Reliability Conference (ESREL 2017).

Naked-science (2017). Как устроена атомная подлодка https://naked-science.ru/article/tech/kak-ustroena-atom naya-podlodka.

NIST (2012). Guide for Conducting Risk Assessments—Information Security (SP 800–30 Rev.1), National Institute of Standards and Technology (NIST), Gaithersburg, Sept. 2012.

SBA (2013). Recommendations for Business Continuity Management (BCM), Swiss Bankers Association, Bale, Aug. 2013 http://shop.sba.ch/999925_e.pdf.

Viperson (2001). *Interview*: Гость программы – Контр-адмирал в запасе Валерий Алексин http://viperson.ru/articles/gost-programmy-kontr-admiral-v-zapase-valeriy-aleksin.

VK (2017). *Video footage*: Официальная версия в фильме о катастрофе АПЛ Курск. https://vk.com/videos543641?z=video61207156_456239177%2Fpl_543641_2.

Гибель “Курска” (2015). *Snipping from Video footage*: Гибель Курска. Следственный эксперимент (2015)
https://www.youtube.com/watch?v=INJTLXL5GrQ&has_verified=1.

Рязанцев, В. 2017. В кильватерном строю за смертью. Почему погиб «Курск». ISBN: 978-5-906716-88-0.