PROFOUND DECISIONS IN DANGEROUS SITUATIONS OF SMALL AND MEDIUM-SIZED ENTERPRISES. A "LESSONS LEARNED" IMPULSE FOR SME MANAGEMENT OF RISK AND UNCERTAINTY TO AVOID DISASTERS

DIRK C. PINNOW

DOI: 10.26410/SF_1/21/2

ABSTRACT

SMEs – often run as family businesses with full existential risk – are considered the "backbone of economy" in German-speaking countries and pillars of prosperity. With respect to their economic importance, they need help to minimise risks, master crises and avoid catastrophes. The current Corona crisis endangers those SMEs in particular, which address end customers with direct contact to sell products or provide services. There are in general numerous existential threats, both physical (break of supply chain) and virtual (cyber attacks on availability, integrity and confidentiality of IT and OT systems). Since managing directors of SMEs are often still involved in everyday business and many tasks are performed in personal union, risk management rules that address larger, stock exchange listed companies are at best suitable for inspiration – bureaucracy and low practicability in everyday SMEs' life could be an unwanted result of 1:1 application as an end in itself. "SME captains" who are also practically active in everyday life needs pictorial, easily comprehensible instructions on risk and safety / security management with a high practical relevance. Since they see at least their ideal and also socio-economic existence threatened in the event of failure, it is advisable to cite sufficiently detailed investigated and evaluated incidents – e.g. accidents or near major loss events – as striking examples and to derive recommendations from them. In this article, selected incidents from aviation and military are considered as cautionary and insightful interdisciplinary examples of basic mental and organisational preparations for crises and transferable findings are derived for SMEs, which may help to avoid catastrophes. Even simple organisational preparations and appropriate methods can help to establish an SME early warning system, far from being an end in itself, can increase the resilience and enable the successful application of an emergency and recovery plan.

KEY WORDS

Aviation, idyll, decision, military, risk, safety, security, SME, sustainability, uncertainty.

DIRK C. PINNOW, DIPL. ING.
e-mail: dirk@pinnow.com
Berlin General Conference of Safety
and Security Institutions (BGKdSI)

Distrust the idyll
She's a killer scrap -
If you take her side
She'll beat you back!
(1st verse of André Heller's "Emigrant's Song", own translation)

Introduction

In his "Emigrant's Song"[1], the Austrian artist André Heller addressed the dangerous underestimation of the supposed idyll and also used this motif in his flower arrangement for the Federal Garden Show 1985 in Berlin: a colourful group of flowers, seemingly banal from the ground, only showed the viewer the warning *"Distrust the Idyll"* and a jester's face[2] above a labyrinth after climbing a lookout tower. In this sense, decision-makers, especially in SMEs, should be presented a corridor of action between downplaying and routine negligence on the one hand and fatalism or hysterical fearfulness on the other. In the following, the author gives an impulse with suggestions for SME management, which are derived from findings from tragic accidents and real, potential doomsday scenarios. In the course of their work, SMEs very often find themselves in crises – i.e. in acute, disturbed operational situations that require timely, directional decisions in order to maintain resilience and return to a stable state.

Business administration (BA) offers entrepreneurs approaches to solutions in three categories[3] by means of the Decision Theory: decisions under certainty, decisions under uncertainty and decisions under risk. Accordingly, a decision[4] is understood as an action that selects from several alternatives the one that promises to best serve the achievement of the goal – i.e. the current state (e.g. a dangerous situation) is to be transformed into a desirable state (e.g. minimisation of danger). For decisions under uncertainty, mathematical methods (e.g. the "minimax rule") are offered to reach mathematically justified decisions despite a lack of probabilities of occurrence – for example in the calculation of sales prices. This is now very much a factor in the success of a company and can also threaten its pure existence if the wrong decisions are made. In this article, however, the focus will be on entrepreneurial decisions in the face of situations in which uncertainty and risk interact and the threat to the company's existence is more serious than just in the case of unsuccessful pricing:

Not only the integrity and continued existence of the company is at risk (security breaches), but also the health / integrity, property rights or reputation / dignity of people (shareholders, employees, customers, neighbours) are threatened (safety breaches).

Such threat scenarios are characterised either by a lack or flooding of information, by a restriction or focussing of perception, often in combination with distraction or even confusion. For companies, there are numerous obligations

[1] The entire lyrics can be found at https://genius.com/Andre-heller-emigrantenlied-lyrics.

[2] An impression of the flower arrangement is shown here: https://www.andreheller.com/portfolio/labyrinthe blumenbilder-und-garteninstallationen/.

[3] *"In decision theory, decisions under uncertainty are decision-making situations in which the probabilities of occurrence of future environmental states are not known".*

[4] *"Decision theory aims to provide assistance in making 'good' decisions. It can be divided into prescriptive and descriptive decision theory".*

and procedures for the management[5] in order to maintain safety and security in a targeted manner in all operational phases – thus, appropriate and safety-and-security-compliant operating regulations should be planned, applied and observed at all times, in regular as well as in replacement operations.

Consultants with practical experience, especially in the smaller companies of the so-called small and medium-sized enterprises (SMEs), will have experienced how difficult it is to address managing directors or board members with theoretical approaches and abstract management methods and to persuade them to change their behaviour in the long term.

In the following, an interdisciplinary approach is chosen to provide *"corporate leaders"* or *"masters in their own house"* with the most practical experience possible from aviation and military, in order to be able to make decisions in crises, despite unclear information, which prevent the occurrence of a catastrophe, temporarily place operations on a fallback level ("fail-operational") and allow normal operations to be restarted soon.

1. Limited perception

As human beings, all decision-makers are fallible and thus limited in their perception of reality. In times that are perceived as banal everyday life, there is a danger that suddenly occurring disturbances (obstacles, adverse circumstances or even dangers) are filtered away, i.e. are not even consciously perceived.

A good example of the realisation of limited perception (target focussing) is the attention experiment depicted in several film recordings[6], in which the video viewer is asked to count the number of rallies between members of a team dressed in white, whose movements on the playing field are mutually interspersed by those of the "black" team.

All attention is now mostly focused on the ball game of the "white" team and the counting is done with exertion – those who pay close attention come up with the correct result of 15 rallies. But the result is not so important: The viewer is now confronted with the question of whether she or he has also seen the man in the gorilla costume.

Nearly anyone who has not seen this video before will be very surprised, but then the sequence of rallies is repeated and indeed, in between the both teams an adult person dressed as a monkey can be seen prancing between the ball players from right to left.

This example may amuse, but it can also frighten. For example, anyone who drives with a car to work every weekday on a road with a speed limit of e.g. 50 km/h could one day have a disturbing key experience when suddenly – perhaps even in a bend – the speed limit has unexpectedly been lowered to 30 km/h because this section of the road poses a potential danger due to a roadworks site with lane narrowing that was just set up shortly before.

Anyone who always drives responsibly will probably master this seemingly banal challenge without danger. But if, in addition to the filtering of perception caused by previous everyday experiences, a so-called target focus (*"just be on time!"*) is added, there may even be a danger to life. There are enough examples of tragic outcomes in aviation:

[5] Management procedures are an *"indispensable prerequisite for generating and maintaining safety"... "For operations, it is essential that appropriate and safety-compliant operating procedures are planned, applied and observed at all times."* The same applies to security!

[6] This experiment is shown in a number of variations – sometimes the result of counting is different and in some cases in addition the colour of the background is changing.

A fatal accident e.g. occurred during a flight of the Swiss airline Crossair from Berlin-Tegel to Zurich-Kloten on November 24th in 2001[7]. The route was well known to the two pilots, but that evening there was snowfall mixed with rain, it was late and the desired runway with an Instrument Landing System (ILS) was not available.

The pilots, apparently also driven by the desire to land on the first approach and get home quickly[8], steered the aircraft into a descent without ground visibility until it struck trees and crashed into the forest five kilometres apart from the runway – a fatal crash (24 of the 33 occupants died, including both pilots) was the result.

These examples before may suffice to show in analogy the dangers for managing directors and board members of small and medium-sized companies – their wrong decisions due to filtered and misfocused perception may not cause any fatalities, but idealistic and economic livelihoods can always be destroyed though:

- An "internal perpetrator" may be up to mischief in the company in the sense of industrial espionage, theft / fraud, hacking / sabotage and remain unnoticed because the security precautions were only designed for external threats.
- In another case, the repeatedly postponed market launch of a new product with dubious prospects of success is grimly persisted, for so many resources have already been invested in it that success is to be forced *"at any cost"*, even if this robs other branches of the company of valuable potential.

Apparently, in such cases, insufficient or non-targeted and cautionary information is deliberately available to the decision-makers.

2. Overestimation and time pressure – air crashes of Tenerife and Überlingen as a lesson

On the runway of Los Rodeos Airport in Tenerife, a Boeing 747 of KLM Royal Dutch Airlines (KLM) collided with a Boeing 747 of Pan American World Airways (Pan Am) on March 27th in 1977 – 583 fatalities were the terrible result[9].

Both had taxied one behind the other on the single runway in very poor visibility, as the actual parallel taxiway in the apron area was occupied by parked aircrafts. Language misunderstandings regarding the take-off clearance and the time pressure for the KLM crew led to the Dutch initiating the take-off, although the Pan Am Boeing 747 – which shortly before had ignored an exit to the taxiway running at an acute angle (in order then to line up behind the KLM aircraft for take-off) – was still approaching on the runway in the fog and could not sidestep quickly enough to avoid the collision. This accident is considered one of the most serious in civil aviation and to this day the most serious ever without a terrorist background. It shows a fatal combination of error factors on the part

[7] *"According to the Swiss Bureau for Aircraft Accident Investigation (BFU), the main cause of the accident was falling below the minimum descent altitude".*

[8] Peter Klaus Brandl, professional pilot, flight instructor, management trainer and author, devotes his books and lectures to gaining knowledge from aviation incidents and deriving recommendations for managers. His comment on this accident: *"Never, close your eyes and get through it'! Especially shortly before the goal: Keep your eyes open and concentrate! Be ‚go-around-minded' until the end – be prepared, for example, to postpone a business deal or a negotiation".*

[9] The KLM aircraft took off without clearance and collided with the Pan Am plane still taxiing on the only runway. *"Contributing factors to the accident were impaired visibility due to dense fog and inadequate and misleading communication between the KLM pilots and the ground control in the tower".*

of those involved (KLM and Pan Am as well as the tower), which together determined the perception and decision-making, especially of the captain of the KLM Boeing 747, and ultimately led to the catastrophe:

- The previous diversion of air traffic to Tenerife due to a bomb attack and another threat in Gran Canaria was actually a deviation from routine – as were the poor visibility conditions – and should have immediately sharpened the attention of all involved (controllers and cockpit crews alike) to unexpected challenges.
- The airport was not familiar to the diverted crews of KLM and Pan Am (these were special flights) and not really suitable for aircraft of this size – particularly careful navigation on the only runway, especially in the limited visibility (fog), with repeated explicit reassurance for take-off clearance, would have been required.
- The blind trust in one's own abilities and the focus on the goal of getting back to Amsterdam on time without exceeding the maximum service time apparently created the illusionary perception in the KLM captain's mind that he had already received the take-off clearance from the tower and now had a free runway in front of him.

This tragic example could be taken as a warning – literally written in blood – for companies as well:

(1) Even the banality of everyday routine must be distrusted and met with the utmost attention; but when a serious deviation from routine occurs as a result of an unexpected incident that causes diversions or delays and at least temporary transitions into a previously unknown environment, perception should be sharpened even more than ever. Those who have been operating unchallenged in a "daily routine" for a long time will possibly try, in the sense of pattern recognition, to find familiar, ingrained patterns even in this new environment and largely proceed as usual. In such a situation, however, decision-makers should feel more like cautious "pioneers" in a kind of a dangerous "new world", open their perception wide and proceed even more stringently than usual according to "standard operating procedures" (e.g. in the form of checklists) for operational elementary functions that remain unchanged even in exceptional cases.

An example: Even in the case of great time pressure, for example as a result of a disruption in the supply chain, goods or equipment arriving at the factory should still be checked as usual for type, quantity and quality and transferred to the store with a documented stock entry. Not doing so – because it has to be done *"quickly"* – would violate a security feature that is too often underestimated, namely that of availability. The non-availability of complete data for the enterprise resource planning and accounting system can cause unexpected problems, for example with the tax office, if the current assets of raw materials and supplies, semi-finished products or finished goods cannot be shown in the balance sheet in an audit-proof manner. Calculations based on unclear stock levels could also cause errors and thus damage.

(2) If a commercial enterprise, especially an SME, enters a previously unknown field, such as a new sales territory abroad, then the greatest care should be taken in communication. Differences in culture, language and legislation offer numerous pitfalls – in oral agreements and even written contracts (e.g. a Letter of Intent / LoI or an extensive detailed

treaty) it must be worked out what the different partners understand by the chosen terms against the background of their cultural character.

For example, it makes sense to agree on a common language – in foreign trade this will often be English – and to refer to internationally proven, clearly defined standard procedures, such as those described by the so-called "Incoterms"[10]: These regulate, among other things, the assumption of costs and responsibility for the international transport of goods (the so-called transfer of risk), the place of delivery or takeover, questions of insurance, customs clearance and documentation.

(3) Decision-makers should set clear criteria for minimum requirements in order to decide whether to start a particular process, postpone it or abandon it completely.

An example: A new machine tool to be integrated into the Internet of Things and Services is soon to be exhibited and even demonstrated at an industrial trade fair. The stand has already been booked. A deadline should now be set by which the prototype must have a presentable minimum functionality – or not. To avoid reputational damage, the machine should only be reliably demonstrated to expert trade fair visitors. If this still seems too uncertain, no press release should be sent out to raise false expectations, but instead the very concept should be presented at the trade fair by means of animations, display boards and, if necessary, models – with a reference to the *"intensive testing currently underway"*. This way, the company could be spared an embarrassment and at least collect contact data of interested future customers and media representatives.

The accident in the airspace near Überlingen on Lake Constance on July 1st in 2002[11] also illustrates how unfortunate circumstances can chain together to lead to disaster. The collision of a DHL Boeing 757 with a Tupolev Tu-154M of Bashkirian Airlines from Russia claimed 71 lives, including 49 children.

- The Russian aircraft had taken off as a special flight with a one-day delay. On the evening of the accident, the private air traffic control company Skyguide in Switzerland, which was also responsible for monitoring the airspace of the Lake Constance region for the German part, was undergoing maintenance – the telephone system was not working, so that it was not possible to contact German colleagues.
- Due to the expected low traffic during this night, one air traffic controller dared to monitor two spaced radar consoles alone at the same time and sent his colleague on an unscheduled break.
- Although both aircrafts had a functioning anti-collision system (Traffic Alert and Collision Avoidance System / TCAS), the priority of instructions was not clear at the time. An analogy from road traffic may help to understand the decision-making priority: According to the German Road Traffic Regulations (StVO), for example, a traffic policeman's instructions on the right of way at intersections have priority – regardless of what the traffic lights or signs indicate at that moment. Thus, although the TCAS indicated otherwise, the Russian pilot followed the control-

[10] The term stands for "International Commercial Terms" and refers to a set of predefined international rules published by the International Chamber of Commerce that define contract terms for international commercial contracts. *"Incoterms play a very important role for international sales contracts".*

[11] For years, Skyguide had accepted that only a single controller was on duty during the low-traffic night hours.

ler's instructions, descended like the DHL plane, and the disaster took its course – only after this accident was it established that, in principle, the TCAS instructions have priority.

Instructions for companies can also be derived from this fatal accident:

(1) This crash also underlines that the supposed "idyll" of banal everyday life should be fundamentally mistrusted and no slackening of safety standards should be permitted. If unexpected deviations or developments occur, sudden crises must be expected, which can slide into catastrophes through misconduct or omission.

An example: It happens from time to time that excavators accidentally cut supply lines (electricity, telephone, water, gas) without warning during construction works, thus surprising consumers in the vicinity in an unpleasant, harmful way. Every manufacturing company should deal with such a scenario in good time in order to provide for fallback levels ("fail-operational") at least for emergency operation. Otherwise, there is a risk of damage even to the machinery (e.g. in galvanising baths, plastic spraying plants, foundries, etc.) or possibly delays in the completion of an important order of existential importance for the SME concerned, which could be subject to a penalty for non-performance.

(2) In supervision tasks in the sense of monitoring and control, (diverse) redundancy should be used, even if the upcoming shift or a process seems to run calmly and undisturbed.

Example: In the control room of a waterworks facility, several monitors have to be kept in view – among other things, the quality of the drinking water has to be continuously monitored. Just because there is no major television event coming up that evening, such as the final match of a football World Cup, during whose half-time break a sudden increase in demand is to be expected, a deviation from the supposed – calm – course should be expected at any time. If a member of staff then has the confidence to keep an eye on all the monitors and also the screens for video surveillance of the site alone and willingly sends his colleagues off for a longer cigarette break, in the event of a crisis there is a risk of disaster due to distraction and excessive demands: If the waterworks facility is located on a lake, for example, carefree youths could try to climb over the fence in order to take a bath in the lake at night. While such an incident attracts the full attention of the employee who is on duty alone and his colleagues cannot be reached at short notice because they have not taken their mobile phones with them, at the same time an oil tank lorry could be driving illegally on a shore road and have an accident there. The oil seeping into the soil near groundwater wells would pose a great danger to the drinking water supply of the surrounding area. Depending on how the alarm system is designed, the control room staff is warned. But what if the staff member who is only actively on duty there is distracted by the intruders and possibly even deactivated the acoustic signal because of too many false alarms recently? This must not happen, but it could.

(3) Every company is strongly advised to have an early warning system for crises as well as a tried and tested emergency and recovery plan – in order to avoid a catastrophe. To a certain extent, this should also define the order of precedence of the right to issue instructions (a kind of a chain of command), which does not have to follow the usual, everyday hierarchy, but ideally should be

based on substitution arrangements in a crisis team organisational chart.

For example, a factory located in an industrial area on the banks of a river prone to flooding has assigned a staff person to keep a constant eye on the water levels of the river in question from the spring, as well as notifications from the authorities and the weather forecast. This person would be then the expert on flood issues in this plant, if he or she takes this task seriously, methodically and responsibly – this person could have the decision-making responsibility in the crisis team in case of an imminent flood and set the emergency and recovery plan in effect.

3. SMEs are always to be prepared to take risks: The Risk Readiness Condition

Without wanting to martially equate the activities of a company in the market with an act of war, it is nevertheless possible to borrow advice from military orgware for civilian applications. Those who do not want to face crises with catastrophic potential unprepared and emotionally, but in a tried and tested, methodical and well-founded manner with a crisis team, could establish a kind of continuous hazard potential analysis according to the principles of a utility value analysis, which is fed by constantly collected key figures and which all those responsible regard every day. Based on this, a signal system similar to the “DefCon” classification (Defence Readiness Conditions)[12] of the US military could be set up.

The five DEFCON stages (according to Wikipedia):

- DEFCON 5 – peacetime;
- DEFCON 4 – peacetime, heightened intelligence and security measures;
- DEFCON 3 – increased readiness, standard radio call signs of US troops are replaced by secret call signs;
- DEFCON 2 – increased readiness, reserve mobilisation;
- DEFCON 1 – maximum operational readiness, all available troops are deployed.

For example, a kind of "Risk Readiness Condition" (RiskCon) could be defined for civilian operations, which would help management and division heads to make decisions on risk management even when the facts are incomplete, i.e. when there is uncertainty, on the basis of guidelines that would also precede the explicit emergency and recovery plan.

Five operational RiskCon levels for crisis phases (author‘s proposal):

- RiskCon 5 – Everyday operations on mundane working days (example: All systems in a bio-chemical laboratory are working perfectly; no significant external threat or influence discernible).
- RiskCon 4 – Everyday operations, recording of non-ordinary malfunctions and checking as well as, if necessary, tightening of security measures (example: The IT manager notices an increased influx of spam mails, so that the intrusion of malware or phishing must be prevented).
- RiskCon 3 – Increased attention, the crisis team receives advance information (example: Above-average water levels are reported from the headwaters of a river at risk of flooding, which is located in the vicinity of the company premises, and rainfall is to be expected in the coming days – if necessary, holiday planning would have to be adjusted in order to have

[12] The highest state of alert ever declared by the US military has been DEFCON 2: During the Cuban Missile Crisis, the Strategic Air Command (SAC) switched to DEFCON 2 on October 23rd in 1962.

the planned crisis team ready for action on the company premises if necessary).

- RiskCon 2 – Increased attention, convening of the crisis team (example: A company in the food industry is accused in social internet networks of delivering harmful products – and the spread of the rumours does not decrease for the time being, there is even a threat of a adoption by regular media. Even if it is still low-level, the crisis team has to take countermeasures promptly – e.g. by sending a message to the media with the test certificate of a testing laboratory).
- RiskCon 1 – Maximum readiness, all necessary resources are kept ready - the crisis is approaching its peak and threatens to become a disaster (example: A fire has broken out in the separate materials warehouse of a manufacturing company – the fire brigade has been informed and is already on site with emergency forces. It is still unclear whether harmful substances will be released and the fire will spread to other parts of the plant. The first sections of the emergency and recovery planning come into effect - alternative rooms for the management are rented from an office service provider; rented lorries are ready to move valuable documents and equipment out of the potential danger zone with the help of the assembled staff, following the evacuation plan).

However exemplary the respective company or business may behave, the decision-makers are either overwhelmed by a flood of information or the resources for detailed data collection and evaluation are not available, e.g. due to the extent of the impending disaster and lack of time reserves. They therefore usually have to make decisions in the face of uncertainty – but the methodology helps them to make obvious decisions based on “best practice” without emotional overload and fatal target focussing.

As part of sensible emergency and recovery planning, checklists that have been tested and, if necessary, modified should be kept on hand on a regular basis. These are not an end in themselves, but should be strictly adhered to – assuming a suitable degree of maturity: They serve as guidelines, provide support, define the framework for decisions and also serve as documentation for subsequent evaluation.

4. Standard Operating Procedures for SMEs

Standard Operating Procedures (SOPs) are used in aviation, for example, in the form of checklists before the actual main process is carried out. They represent *“a binding textual description of the sequences of operations, including the checking of results and their documentation”*[13] – especially for critical operations with potential impacts on the environment, health and safety.

An SME SOP could thus in principle have the following structure (author‘s proposal):

(1) Goal and purpose: What is to be achieved and why?

Example: Enactment of the Emergency Response and Recovery Plan as amended on mm/dd/yyyy to manage operational crises and prevent disasters – specifically, the part for managing a ransomware attack comes into effect.

[13] An SOP usually includes a unique identifier, a validity date or period, a version number and the name of the creator, the approving person within the organisation, possibly the official reviewer and the releasing person with their respective signatures.

(2) Application area: Definition of the operational area?

Example: Exact – clarification whether only valid for the main premises or all dependencies, branches and also external premises. As with a law, the spatial and temporal validity would have to be defined.

(3) Description of the process: How and with what will the activity be carried out?

Example: All operational decision-making levels are informed by eMail and SMS, if necessary also by loudspeaker announcements (diverse redundancy!) about the entry into force of the emergency and restart plan – previously prepared information on behaviour in the crisis phase also goes to the rest of the workforce in these ways. Clearly defined acoustic signals could also be used to sharpen attention and show the seriousness of the situation – recommended in any case in process engineering, biochemical or explosion-hazardous operating areas, where increased time pressure forces immediate action.

(4) Responsibility and qualification: Who is responsible and who is allowed to carry out?

Example: The "Fire Protection Officer" assigned to the executive board as a staff member or one of his two deputies (who may never be on holiday at the same time or must be on call at short notice) take the lead in the event of a fire outbreak to coordinate with the fire brigade and rescue services, if necessary also with the environmental authority. The clear goal is to quickly contain the fire that has broken out, to prevent it from spreading as well as to minimise damage and to initiate evacuation measures (personnel / material). All three selected persons regularly participate in further training (e.g. of the employer's liability insurance sssociation) and have acquired current certificates.

(5) Documentation: What was done when, where, how and by whom?

Example: A virus scan was carried out on the managing director's PC on mm/dd/yyyy at hh.mm o'clock by the IT appointee N.N. using the software "Xyz" – suspicious files were removed.

The documentation of the respective process should be done according to the principle *"the more critical to success, the more detailed"*. The six-eyes principle is recommended for the creation of an SOP, its review and subsequent approval. Those affected by an SOP must be informed and trained. The accompanying SOP change management should serve to modify or optimise the documentation – also with subsequent information and training of those affected.

5. Lessons from the crisis year and near-war year 1983

At the beginning of the 1980s, in the so-called Cold War between NATO and Warsaw Treaty states, the confrontation and misinterpretation of the behaviour of the opposing side came to such a climax that both military blocs accused the other of planing to attack them with nuclear weapons.

In the then Soviet Union, the KGB intelligence chief Yuri Andropov (later head of state from 1982), under the impression of the traumatising German invasion in the Second World War ("Unternehmen Barbarossa"), introduced the RJAN programme (РЯН, short for Ракетно-Ядерное Нападение / Raketno-Jadernoje Napadenije / "nuclear missile attack")[14], which

[14] Due to the NATO manoeuvre "ABLE ARCHER" held for ten days in November 1983, the security situation became even more critical, for intelligence analysts assumed that this event finally could be the feared attack.

was intended as an early detection system to gather information on an expected surprise first strike by the West.

Thus, agents of the Eastern bloc were to report unusual occurrences in NATO countries that could serve as preparations for war – these included, among other things, holiday suspensions, switched-on lights in ministries and at NATO headquarters or calls for blood donations. The agents, financed with expensive foreign currency, delivered information as expected, e.g. that the lights were still on at night in an observed office wing in Brussels – but without checking whether office work was actually being done or whether the premises were just being cleansed by a cleaning brigade outside office hours. All such indications were entered by evaluators into a criteria matrix: Every report, e.g. about holiday cancellations for doctors, was evaluated and entered as an indication of an imminent attack. In this way, the supposed threat image became more and more dense – and with it the willingness to anticipate the presumed attack by the West, if necessary.

Two incidents in particular brought humanity at that time, at least in the northern hemisphere, to the brink of annihilation through a war with nuclear weapons initiated on the basis of false assumptions.

- Thus, the NATO manoeuvre "ABLE ARCHER"[15] in November 1983 for the Soviet side turned out to be an assumed cover for the West's attack. Several errors of perception on both sides of the East-West conflict brought the earth to the precipice: The Soviet secret service KGB, for example, did not recognise the NATO simulation of "DEFCON 1" as such, but interpreted it as actually being on the highest alert (see above) and suspected an attack on their anniversary of the "November Revolution" because the upcoming celebrations would divert the Soviets' attention. The Soviets then put missiles and fighter planes with nuclear weapons on immediate operational readiness. The West, on the other hand, did not notice the Eastern bloc's fears for a long period of time.
- On the night of September 25th to 26th in 1983, the yet Cold War had already come to such an extent that the world was only minutes away from the launch of Soviet nuclear-tipped intercontinental ballistic missiles – as a supposed counter-attack by the USSR following an attack by the USA. Only a prudently acting duty officer, Stanislav Petrov (*"The Man Who Saved the World"*) of the Soviet satellite surveillance in the Serpukhov-15 bunker (about 50 kilometres south of Moscow) is credited with avoiding the ultimate catastrophe for humanity: He believed it was a false alarm when he was notified of the launch of five US missiles in quick succession, because a US nuclear attack would more likely have involved hundreds of missiles simultaneously. *"We are smarter than the computers. We created them,"* he is said to have thought then[16]. The survival of mankind depended on his assessment and report of whether these warnings were false alarms or real

[15] On November 2nd in 1983, "ABLE ARCHER" began as part of the annual autumn NATO manoeuvre, during which a nuclear missile attack on the Soviet Union was practised on a 1:1 scale for 10 days under very realistic conditions. But in contrast to previous years, this time the Soviets registered to their point of view significant, extremely worrying differences.

[16] That night, Stanislav Petrov was the duty officer at an air surveillance centre near Moscow when the computer indicated the launch of five US missiles. He then reported a false alarm to his superiors at the time: *"I didn't want to be to blame for the Third World War"*. Although officer by rank, he saw himself more as a civilian, as educated engineer: *"The world can be glad that I was in command that night – and not a dull military man"*.

warnings, because a Soviet retaliatory strike would have had to be launched before the US warheads hit their targets. According to the German magazine "DER SPIEGEL"[17], in 1983 it was assumed that a war waged with nuclear weapons would have detonated around 5,000 warheads *"over densely populated areas in North America, Europe and Asia"* and would have wiped out *"practically all centres with more than 100,000 inhabitants"*; it was calculated that there would be *"750 million dead and 340 million wounded worldwide"* as a direct result. Petrov's assessment was said to have been confirmed after about 17 minutes by the absence of radar echoes from warheads raining down on the Soviet Union. Later it turned out that *"a sunbeam reflected by a rare cloud formation"* in the reconnaissance system of the satellite "Kosmos 1382" had interpreted the flashes as launching missiles. Otherwise, however, it could have been a total of five intercontinental missiles of the type "Minuteman III", perhaps even equipped with three nuclear warheads each, launched from the "Malmstrom Air Force Base" in the US state of Montana. Petrov, who was on stand-in duty that night, was a trained engineer, a systems analyst with knowledge of the weak points of the technology, and not a *"military machine"* blindly following orders, as was emphasised at the award ceremony for the "4th Dresden Prize"[18] in Petrov's honour on February 17th in 2013.

For decision-making in companies, these two incidents close to World War III touched upon provide meaningful insights and advices:

(1) An operational early warning system for recording and analysing risks must be based on such weighted criteria that can be contextually checked for plausibility and verified. Thus, a risk matrix could be provided with the columns of threat of late delivery, power failure, flood, crime and vandalism, cyber-attacks, fire and severe weather, among others. In the simplest case, suitable employees are designated to regularly sift through information from reputable sources, collect reports relevant to their own company and document them in a way that is clearly visible to the management (e.g. on a whiteboard in the meeting room). For advanced users with an affinity for IT, it is possible to have analysis programmes created and to present the condensed information to the decision-makers online on the screen at any time.

SME Threat Matrix as basis for an early warning system (author‘s proposal)

Threat	**Web sources (examples)**
Fire internal / external	fire alarm centre / fire brigade
Floods	regulatory authorities, waterworks, regional press
Crime and vandalism	police, consumer protection agencies, regional press
Cyber attacks	computer emergency response teams (CERTs), regulatory authorities, consumer protection agencies, IT magazines, police
Delayed deliveries	WHO (see "pandemic"), automobile clubs, overview sites air transport / maritime transport
Power blackout	regional energy suppliers, regional press, social networks
Severe weather	meteorological institutes /services, social networks

Standard values should be available for the assessment of threatening changes: These can be taken from insurance company maps, for example, to assess regional vulnerability to lightning, earthquakes or floods – current police crime

[17] Never has the world been closer to nuclear annihilation than that night, said Bruce Blair, then US disarmament expert and later head of the World Security Institute.

[18] The Semper Opera House, which was heavily destroyed during air raids in 1945, was reopened in 1985: There the award ceremony of the "4th Dresden Prize for Conflict and Violence Prevention to Stanislaw Petrov“ took place, which attracted a great deal of interest, including from numerous representatives of the German armed forces.

statistics should be used to assess the usual threat of crime.

If an analysis indicates an increasing danger, such as rising water levels at the headwaters of a nearby river, the "RiskCon" level should be adjusted accordingly. If, over a longer period of time, there is a clear tendency towards a specific threat typical of the region, for example regular flooding in spring (melt water in the headwaters of the river) and autumn (persistent rainy weather), which cannot be satisfactorily averted by protective measures in the form of barriers, the location of the business should be reconsidered and a move discussed.

The case of Stanislav Petrov also points to the cultural dimension of risk or safety management. Petrov made his level-headed decision in the face of the greatest uncertainty, relying on his intuition, under great time pressure. He stood by his 50-50 assessment of *"false alarm"*, although the technical systems reported an attack five times in succession and the total of up to 15 warheads could have destroyed just as many major cities in the then Soviet Union. He literally saved the world and yet had to accept the end of his career for it.

For companies, the recommendation can be derived from this to appoint personalities for their own operational risk and security management who have the courage to make decisions that are uncomfortable or (initially) even incomprehensible to the management – in the sense of a balance between the protection goals of *safety* (people, internal / external) and *security* (company and branches) in the context of the time dimension (*sustainability*) as well. Mere yes-men as uncritical recipients of orders, who perhaps let the regular fire protection exercise in the company pass just as an annoying compulsory appointment without anyone gaining any purposeful lesson from it or being seriously prepared for a real emergency, may flatter the self-image of a supposedly infallible company leader. But a real severe incident – which can be initiated by even the smallest disturbance in the operational process – could put the management, the owners and the entire company out of business (temporary or even for good).

6. Conclusion: Gaining "strategic depth" through controlling and methodology

The expectations of stakeholders as well as the public, but also the further development of jurisprudence, should make managing directors and board members aware of the necessity to implement a methodically structured and documented risk and security management.

For example, the government commission "German Corporate Governance Code" recommends that in order to ensure *"good and responsible corporate governance"*, supervisory boards should deal with the risk management system of the supervised company[19] – even though currently this recommendation applies to companies listed at a stock exchange yet, which have had the DIN ISO 31000 standard for implementing effective risk management at their disposal since 2018, managing directors of smaller companies should also become active, before it becomes obligatory.

It is to be expected that in the course of legal disputes in the future these benchmarks will also be established more and more as comprehensive standards and

[19] The DIN ISO 31000 standard helps to identify, analyse and evaluate risks so that they can be dealt with appropriately.

will also find their way into contracts as a quality feature (market expectation / state of the art and science). Whether the DIN-ISO standard is strictly followed in a formalised manner or whether an individual system is established that is better adapted to one's own needs is up to the respective SME – but there is no way around such a system!

In order to avoid the escalation of crises and the occurrence of catastrophes, small companies should also implement an early warning system that consistently provides the company management with a resilient, forward-looking control instrument in order to manage operations at temporary fallback levels ("fail-operational") and minimise damage despite remaining uncertainties, supported by checklists as well as emergency and restart plans.

SMEs also need "strategic depth" to limit and mitigate damage effects. In three-dimensional physical space, the possibilities are limited and essentially dictated by the size of the plot and the permissible construction height of the buildings, but the optimisation of processes (such as logistical requirements, enabling short escape routes) also sets narrow limits there. This leaves time as a dimension, i.e. despite time pressure, early detection, training and methodology should be used to create enough "temporal strategic depth" to prevent accidents from occurring in the first place, or at least to allow enough time for emergency and restart planning to take effect, for the crisis management team to be set up and for rational decision-making to take place – freed from both hysteria and target focussing. From aviation, the example of a "go-around" always should be kept in mind.

For a small or medium-sized company, its failure might not mean the biological death of the owner, but it does mean an ideational disaster and possibly also socio-economic hardship, which can threaten very much the pure existence, too. SME decision-makers are therefore called upon to at least be inspired by the risk and safety / security management methods of larger companies and institutions and to implement a system that suits their needs and is reliable in everyday operations – it can help them to stabilise and save their own existence!

Bibliography

Genius Media Group Inc., *Emigrantenlied / André Heller / Album Basta*, GENIUS, https://genius.com/Andre-heller-emigrantenlied-lyrics [accessed April 25, 2021].

Schroer K., *Entscheidung unter Unsicherheit*, BWL-LEXIKON.DE, https://www.bwl-lexikon.de/wiki/entscheidung-unter-unsicherheit/ [accessed April 25, 2021].

Schroer K., *Entscheidungstheorie*, BWL-LEXIKON.DE, https://www.bwl-lexikon.de/wiki/entscheidungstheorie/ [accessed April 25, 2021].

Stephan U. & Schulz-Forberg B., *5.1.4 Organisation des sicheren Betriebs*,VDI-Buch „Anlagensicherheit", Springer Vieweg, Berlin 2020, 311

Simons D., *selective attention test*, YouTube, https://www.youtube.com/watch?v=vJG698U2Mvo [accessed April 25, 2021].

Wikimedia Foundation Inc., *Crossair-Flug 3597*, Wikipedia, https://de.wikipedia.org/wiki/Crossair-Flug_3597 [accessed April 25, 2021].

Brandl P.K., *Das Crash-Beispiel: Zürich, November 2001*, CRASH KOMMUNIKATION – Warum Piloten versagen und Manager Fehler machen, GABAL Verlag GmbH, Offenbach 2010, pp. 75-78

Wikimedia Foundation Inc., *Flugzeugkatastrophe von Teneriffa*, Wikipedia, https://de.wikipedia.org/wiki/Flugzeugkatastrophe_von_Teneriffa [accessed April 25, 2021].

Cargoboard GmbH & Co. KG, *Was sind Incoterms?*, cargoboard. https://cargoboard.de/logistik-abc/incoterms/ [accessed April 25, 2021].

Wikimedia Foundation Inc., *Flugzeugkollision von Überlingen*, Wikipedia, https://de.wikipedia.org/wiki/Flugzeugkollision_von_%C3%9Cberlingen [accessed April 25, 2021].

Wikimedia Foundation Inc., *Defense Condition*, Wikipedia, https://de.wikipedia.org/wiki/Defense_Condition [accessed April 25, 2021].

Wikimedia Foundation Inc., *Standard Operating Procedure*, Wikipedia, https://de.wikipedia.org/wiki/Standard_Operating_Procedure [accessed April 25, 2021].

Wikimedia Foundation Inc., *RjaN*, Wikipedia, https://de.wikipedia.org/wiki/RJaN [accessed April 26, 2021].

Kompa M., *Die RYAN-Krise – als der Kalte Krieg beinahe heiß geworden wäre / Vor 25 Jahren war die Welt näher am Nuklearkrieg als je zuvor oder danach – ohne, dass es jemand merkte.,*TELEPOLIS, https://www.heise.de/tp/features/Die-RYAN-Krise-als-der-Kalte-Krieg-beinahe-heiss-geworden-waere-3420663.html [accessed April 26, 2021].

Leffers J., *Sowjet-Offizier Petrow ist tot / Der Mann, der die Welt rettete*, DER SPIEGEL, https://www.spiegel.de/geschichte/stanislaw-petrow-der-mann-der-die-welt-rettete-ist-tot-a-1168721.html [accessed April 26, 2021].

Bidder B., *Vergessener Held / Der Mann, der den dritten Weltkrieg verhinderte*, DER SPIEGEL, https://www.spiegel.de/geschichte/vergessener-held-a-948852.html [accessed April 26, 2021].

Pinnow D., *4. Dresden-Preis für Stanislaw Petrow: Computermeldung als Fehlalarm klassifiziert und die Welt gerettet / Überfällige Würdigung für einen Ingenieur mit Mut, Herz und Verstand*, datensicherheit.de, https://www.datensicherheit.de/4-dresden-preis-fuer-stanislaw-petrow-computermeldung-fehlalarm-klassifiziert-welt-gerettet [accessed April 26, 2021].

Herdmann F., *Risikomanagement als Basis für gute und verantwortungsvolle Unternehmensführung*, DIN Mitteilungen +elektronorm ZEITSCHRIFT FÜR DEUTSCHE, EUROPÄISCHE UND INTERNATIONALE NORMUNG, Ausgabe Januar 2021, pp. 22-25.

About the Author

Dipl.-Ing. (TU) Dirk C. Pinnow, born 1965 in Berlin, graduated in General Mechanical Engineering at the Technical University of Berlin. After gaining experience as a project engineer in a Berlin computer systems company, among other things with a focus on CAD, he went into self-employed business in 1994 together with his brother, Carsten Pinnow, and has since been active as a consultant, lecturer, speaker and publicist. One of his main focuses is the topic of data security - on this he is the editor of the German web magazine "datensicherheit.de". He is concerned about the survival and success of small and medium-sized value-added structures in so-called SMEs, especially with respect to the Digital Transformation; in this context, he is a founding partner of the Cluster Industry 4.0 (CI4) initiative, too. In honorary engagements, he is the head of the VDI/VDE Working Group on Safety-Security-Sustainability (AKSi) for the VDI District Association Berlin-Brandenburg, a member of the VDI-GPP Technical Committee "Safety & Security" (FA512) and chaiman of the Berlin General Conference of Safety and Security Institutions (BGKdSI).