Chapter 8

Practical Propagation of Trust in Risk Management Systems

Kristian Helmholt, Matthijs Vonder, Bram Van Der Waaij, Elena Lazovik and Niels Neumann

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.70741

Abstract

Using risk management systems for large-scale asset management is not without risk itself. Systems that collect measurement from a geographically diverse area, across many organisations, contain many interacting components that can fail in many different ways. In this chapter these systems are discussed from a risk assessment point of view, using practical examples. It provides suggestions how trust can propagate between interacting components of risk management systems by making information needed for risk assessment information explicit.

Keywords: asset management, systems architecture, uncertainty, trust, distributed systems

1. Introduction

This chapter is about trust propagation in risk management (related) systems used for large-scale asset management that are largely constructed using information and communication technology. An example of such a system is a smart grid monitoring system used for managing the risk of power outage. Based on measurements and failure models, it determines the probability of future failure of components of the grid and the impact of such failure. The focus will not be on the type of risk management these systems were designed to support. Instead, the focus is on assessing risks involved with these systems.

We look at large-scale distributed systems that are so complex that no individual member of the set of people involved in the life cycle (design, construction, operations, etc.) of such a

system can understand the entire system. It would require more study and training from any individual than what could be reasonably expected of a human being. Assessing risk in this context requires the propagation of trust between the collaborating multidisciplinary members of the group. Members can vouch for certain aspects of the system based on their knowledge and expertise but need to rely on each other's judgement to come up with a verdict about the system itself and its output as a whole.

Special attention will be given to (1) automation of propagation of trust and (2) make the trust propagation process itself transparent, so that the system can be studied/audited/inspected by third parties that were not involved either in creating a system (of systems) or in monitoring that system. We work from the assumption that these independent third parties must be able to assure people that a system that supports (or even makes) decisions can be trusted. If these systems fail for whatever reason, it should be detected quickly. We go by this assumption, as we think, that without the ability to have people trust decision support/decision-making systems, these systems are useless in practice. Without these systems our societal toolkit to deal with a growing dependency on relatively scarce resources like energy, fresh water, skilled labour force, etc. is becoming dangerously empty. Dealing with these problems requires effective decisions that take into account analysis of many different aspects of physical reality which is above individual human capacity. We will describe several of those systems that are quintessential in making optimal decisions in societal domains where nonoptimal decisions—let alone failure—are becoming less and less of an option.

We start this chapter by describing cases where risk management (related) systems (should) provide information to decision-makers. There is risk involved in all decisions. The risk (R) is defined as the product of impact and probability of an undesired event/outcome. For example, the decision of an electricity grid operator not to replace an electricity cable might result (probability p) in power outage (undesired event), while at the same time, the decision to replace the cable might result (1-probability p) in unnecessary spending of money. What is 'worse' depends on the valuation of the undesired events, which can be difficult to compute. If, for example, the loss of power (indirectly) results in the death of a person that could not call an emergency number, the impact is huge. Valuation of such impact is not a topic of this chapter, neither is the computation of probability for each case. Instead, after providing a description of the cases, we will show an approach for propagating trust. Last but not least, this chapter is not about specific improvements to fault tree analysis (FTA) or failure mode, effects (and criticality) analysis (FME[C]A).

2. Examples of trust propagation in risk assessment

In this section we provide examples of risk management (related) systems. We will not provide a comprehensive risk assessment of each system as this is beyond the scope of this chapter. The function of these examples is to serve as a backdrop later on in this chapter for illustrating approaches for propagating trust within these systems and to its end-users. All examples are derived from real-life cases on which we have worked. For reasons of clarity, explanation purposes and customer confidentiality, they are not 'verbatim copies' of reality.

http://dx.doi.org/10.5772/intechopen.70741

2.1. Railroad degradation: finding the cause behind the effect

This example serves as a means to show several risks involved in cause and effect relationships in complex systems.

Rail transport operations involve many risks at different levels of abstraction. People depend on the transportation of objects (e.g. people, cargo) to arrive safely within time, possibly comfortable and within budget constraints. End-users run many different risks, for example, not arriving on time, getting killed in an accident, paying too much, etc., different probabilities and different costs of impact. Railroad operators in turn run the risk of creating an accident and delay and providing uncomfortable or overpriced services, etc. In this example we focus on a specific aspect: determining the probability that a specific segment of physical track becomes unavailable due to physical degradation. This probability is a welcome ingredient to sophisticated risk assessment. For example, it can be used to determine when to perform maintenance, or it can be used to determine which tracks are available for routing trains. It is far from trivial to determine this probability, due to the many cause and effect relationships present in railroad operations. This is because of the many physical interactions of objects and forces that together influence the physical condition of the track. These interactions are the results of actions that in turn are the results of processes at different organisations and people involved in railroad operations. For example, an object that exerts influence is the train that interacts with the track through its wheels. The presence of a train is the result of planning of railroad transport carrier organisations. The interaction of the train with the track is influenced by the type of train, its weight, its length and the amount of trains. The track also interacts with its surroundings, like the geotechnical situation (e.g. 'soft or wet soil'), and the weather. The degradation of the track is also influenced by the construction materials, shape and specific construction. Last but not least, maintenance activities influence the degradation process also (i.e. 'it disrupts degradation'). All these influences interact in a way that seems (and probably is) far from trivial to understand. There is a lot of uncertainty with respect to determining the probability of degradation.

In recent years parties involved in railroad operations (i.e. railroad operators, contractors, etc.) have come up with approaches for arriving at a better estimation of the probability of (un) availability of the track. Many of these approaches are based on the idea that future states of the track can be estimated on knowing previous states. This is based on the assumption that a future state is (at least partially) determined by previous states, which can be the case in physical systems. The idea is to analyse recordings of previous states and discover a mathematical relationship between past and present states. This relationship could in turn lead to a prediction/estimation of future states by carrying out computations with previous states as input. From the viewpoint of risk assessment, roughly stated, two types of mathematical relationships can be identified: statistics based and physical model based. The first approach looks at parameters that describe the level of track degradation (e.g. height, shift, etc.) through time. It tries to fit those parameters in a mathematical function that describes the development of the parameters through time as accurate as possible (e.g. 'linear regression', 'curve fitting'). The future state is then estimated using this function. There is no real physical understanding of the system observed. The second approach also looks at parameters that might influence degradation (weather, soil type, etc.). It tries to find a mathematical relationship between

influence parameters and degradation parameters through time, resulting in a physical understanding in terms of a model. If that relationship is well known, the future state can be predicted based on measurement of the previous state, influence parameters and application of the model. In practice there are combinations of both approaches. For example, Bayesian networks can be used to determine the conditional chance that a track will degrade. The idea is to determine the contribution of different influence parameters in the probability that a track will degrade. For example, an outcome of an analysis using Bayesian networks might be 'if 80% of the trains crossing the track travel at a speed of 100 km/h, the probability of severe track height degradation is 65%, where as it is reduced to 30% if only 20% of the trains travel at that particular speed'. Using this approach does not provide a complete physical model, but it does provide a deeper understanding of the observed system when compared to extrapolating on a degradation parameter like height alone. In summary, discovering/determining a physical model is far from trivial in railroad degradation. This is due to the many interactions of potential influence parameters and diversity in track construction and operations.

From the perspective of assessing risk in using an approach like this, several types of risk can be identified. There are risks involving:

1. **Measurement.** For example, the recorded measurement might not reflect the actual physical reality. This can be caused by different things: faulty measurement sensors, errors in recording, errors in converting data during data preparation, etc. Also, measurement methods might change throughout the years. A more accurate set of date might become available with different characteristics. This in turn might result in the observation that 'during the years something changed in track behaviour', while it was only a change in the measurement method.

2. **Analysis.** For example, analysts might assume that a set of measurements is more accurate than it is in reality. Analysis errors might be made due to difficulties in comparing different measurement sources (e.g. height of track, soil saturation of the underground, speed of trains, etc.). As different aspects of reality are measured at different points in time and location (in this case), mathematical interpolation of these types of data is needed for combining them. This might be a wrong conclusion as they are not tightly coupled in and come from complex multivariate and multi-organisational systems.

3. **Persistence of analysis results** (i.e. identified mathematical relationship). For example, if a mathematical relationship has been discovered, while an influence parameter did not change during statistical analysis of measurement data, the model might not take that parameter into account. As soon as this influence parameter changes, the modelled mathematical relationship will probably be no longer valid.

These risks directly translate into trust issues. Measurement experts must be able to trust sensors. Analysis experts must be able to trust measurements. Risk assessment experts must be able to trust analysis results. As all three areas are different areas of expertise, there is a need for propagation of trust. Again, this is far from trivial as railway systems contain thousands of kilometres of track in different surroundings, used in many different ways. Coming up with a methodology (or system that automates this method) that estimates the probabilistic chance of unavailability due to

http://dx.doi.org/10.5772/intechopen.70741

degradation in a uniform way is a challenge. It involves collaboration from different experts working at different organisations at different locations. Each organisation has to be trusted to provide the right information. This can be extra difficult in competitive markets, which is the case in some countries (e.g. the Netherlands). In that market cargo transportation companies compete for cargo, and contractors compete for the right to maintaining track for a period of several years. Sharing data or analysis methods might interfere with the rules of competition. For example, determining the cause of a stop in degradation requires knowing where and when a contractor performed maintenance on the track. This however is also part of the competitive edge a contractor has. This is an impediment to sharing this kind of data in general.

2.2. Pipeline management: trusting a computed future

This example [1–3] serves as a means to show the risks involved in computing possible future states of complex systems.

In the Netherlands distribution of drinking water and gas is largely done through underground pipelines, as the soft soil of most of the Netherlands permits for relatively easy modification of the top (1–2 m) layers of soil. Failure to provide water and gas has a severe impact on economy and society. Risk management is part and parcel of the work carried out by the organisations responsible for the management of these utility networks. They target at minimising risk within budget restraints by spending resources (time, money, etc.) in the most optimal way. Risk assessment constitutes an important part of their activities in minimising risk. In this example we focus on assessing the risk of structurally unreliable pipelines due to the influence of ground settlement. This risk is significant enough to be investigated, as (in the Netherlands) the top soft soil layer can—and does—move at different speeds at different places. This can cause strain in the pipelines, and depending on the materials and specific geometry they can rupture or break, it can result in leakage. Next to not delivering gas and water, there are other types of impact. Water leakage can result in local flooding that can destroy roads ('sinking cars'). Gas leakage might result in explosions that (at least partially) destroy houses as gas seeps into basements from underneath the roads where most pipelines are situated. Risk managers therefor want to reduce as much uncertainty as possible with respect to the probability of this type of pipeline failure occurring.

One approach that is currently being used in a project at TNO is to use physical models of reality to estimate the likelihood of possible future states of pipelines. The following models are used:

1. **Soil settlement**, as a result from the interaction of difference in forces on the ground (e.g. heavy load), geomechanical behaviour of soil types (e.g. clay, sand, etc.), etc.
2. **Forces on a pipeline**, as a result from differences in soil settlement
3. **Mechanical stress in a pipeline**, as a result from forces on the pipeline and its geometry
4. **Probability of breaking/tearing**, as a result from the mechanical stress and the material of the pipeline

The construction and maintenance of these models require specific expertise, for example, in the area of geotechnics and structural reliability. A multidisciplinary team is needed for the constructing a supermodel that integrates all of these models. This 'supermodel' requires a broad spectrum of input parameters, including:

1. Detailed geographical description of soil type
2. Forces on the ground throughout the years, as geotechnical processes can take years (e.g. 30 years for settlement due to a specific load)
3. Location, geometry and material of the pipeline

Information about these parameters is not available in a uniform way. There are drill samples of the soil, but not from all locations. This has to be derived using another model that provides an (probabilistic) estimate of what type of soil could (most likely) be located at a specific spot. Often, there is information about when an area was transformed into a 'built environment', but what exactly was built or deposited when and where is mostly forgotten in history. This has to be derived and estimated from other sources. There are geographical information systems (GIS) containing information on 'where to dig' for pipelines, but the exact height and location are often not known. Not in the least because of the fact that pipelines can move due to the softness of the soil. So, the 'supermodel' has to deal with a lot of uncertainty. This is partially done by including the actual settlement of the top soil layer, as measured by satellites. This data can be assimilated in order to keep estimations of soil settlement closer to reality. How this is done is beyond the scope of this chapter.

Because there is a lot of uncertainty with respect to input parameters, the engineers behind this approach have decided to use 'stochastic modelling'. Roughly stated, it means that not one possible future state is computed using the chain, but many different possible states, based on probability density functions. For several possible variations in a variable, a possible state is computed. Given the amount of variables involved and the different probability density functions, these results in many different possible future states. These are subjected to a statistical analysis, which then results in a 'most probable future'. Note that this approach has only become affordable recently due to developments in the automation of distributed computation. The amount of time to wait for results can now be reduced drastically by computing in parallel across clouds and combining the results later on.

The use of so much input data means that there are risks involved with measurement and (statistical) analysis, just as in the previous 'railroad degradation' example. Other risks are:

1. **Untimely arrival of data.** As the 'supermodel' requires a lot of data on a regular basis to update its estimations, it might be the case that one of the suppliers fails to deliver on time. This will impact the output of the 'supermodel' in the sense that it is an outdated advice.
2. **Inaccurate integrated model of the physical world.** For example, the models might represent a correct understanding of the physical world separately, but when integrated into a 'supermodel', they do not. For example, a pipeline itself might influence the behaviour of the soil too, which might not be taken into account by the soil settlement model.

3. **Incorrect understanding of uncertainty.** Expressing uncertainty with respect to input or a result is far from trivial. If an experts states that his model provides 75% accuracy in settlement, what does that mean? Does it mean that the soil could settle a 25% extra? Or does it mean that 75% of the estimate is spot-on. This has to be communicated in very strict way for proper risk assessment.
4. **Errors in computation.** In order to provide actual numbers, a model needs to be implemented in software to be run on a (distributed) computer (system). The more software is needed to be written for carrying out the computations involved, the bigger the chance that some programmer makes an error during implementation. As the computations are complicated and many, it might be difficult to detect this error.
5. **Errors in presentation.** Finally, if the results are somehow misrepresented on screen or on paper, it is still possible to make the wrong decision.

2.3. Smart grid analysis: non-available data

This example [4, 5] serves as a means to show the risk of data becoming unavailable.

In the Netherlands, electricity is distributed throughout underground low-voltage utility networks, just as water and gas. That makes the cables and their connections invisible to direct visual inspection. However, as the condition of the cable isolation contributes significantly to the risk of power outage, knowledge about the actual state of the isolation is an important ingredient for assessing the risk of power outage. An approach, currently under investigation in research projects, to deal with this uncertainty is to come up with an estimate of the condition of the isolation part of the cable, using a model that takes into account the material of the cable, its construction, its surroundings and the power loads it has been subjected to. This model will be developed based on analysing measurements. Using methods from applied statistics, researchers will try to identify relationships between power outage and specific influence parameters. This approach can be compared to the one used in the 'railroad degradation' example above.

What makes this example different from the previous ones is the possible need for accessing data that is protected by privacy laws. Specific power might influence degradation of the condition of the insulation part of the cable. To determine if this is the case measurement, data is needed on the demand and supply of power to a distribution network. Smart metres (at households) might be able to provide this data. However, this data could also provide insight into what equipment is used at which times of the day. This is why smart metres have been the topic of many heated privacy debates. Smart grid operators might be allowed by special law to only use the data for grid analysis. However, in the future there might be new and tougher laws on privacy that stop the operators from having access. Keeping the system (i.e. failure models) up to date will then become a challenge.

This case shows the risk that data is not (always) available, this time due to the introduction of a law instead of a (temporary) failure of a data supplier to deliver.

2.4. Precision dairy farming: sharing valuable information

This example [6] shows the risks involved in sharing commercially sensitive data.

As dairy farming concerns livestock, it involves many different risks, for example, risks involving food safety and animal health. Assessing risks in detail requires having information on cows, their surroundings, their food, etc. In the past it was difficult to retrieve this information as it was not recorded. But as sensors and ICT have become more affordable, farms are becoming places where a multitude of sensors gather measurement data for interpretation by experts that work on improving milk production, cow welfare, etc. Also, laws and regulations have changed in order to ensure safety and care for the animal and the environment.

The information gathered by these systems however is not easily available for everyone. This is because it provides insight into 'secrets of the trade' and not every animal expert wants to share its findings or data/information. There is the risk of 'teaching your competitors'. Discovering cause and effect relationships requires long-term observation of cows in their contexts. This can be difficult as cows can 'switch farms'. There is the risk of data on a cow being unavailable.

Recently, the InfoBroker concept [7] was developed: 'a platform to make real-time sensor data from different farms available, for model developers to support dairy farmers in Precision Livestock Farming. The data has been made available via a standard interface in an open platform in real time at the individual animal level'. The InfoBroker is designed to making data stored in diverse places available in an efficient and controlled manner. Data is not stored centrally, but remains at the source. The InfoBroker is capable of retrieving individual cow data from many sources while at the same time serving a large number of models on demand. 'For each farm it is specified which data may be released by the InfoBroker. This means that the farmer continues to be the owner of the data'.

Newly identified risks are related to the uncertainty of the quality of the sensor data. Not all data sources are created equal. Some sources are more precise or more frequent (and some change over time). Does a sensor measure the weight per 10 kg or per 0.1 kg? Does a sensor measure the activity per day or per min? For some applications, this is irrelevant. For example, for a dashboard application, typically the data is presented as is, without any qualitative indication. For others, especially model-driven applications, it is essential to know if the data from the device is accurate enough to be used. Some scales can be used as weight input; others are not precise enough. Some activity sensors produce frequent enough measurements; others accumulate over too long time periods. It depends on the farm which sensors are used and therefore available to the model. Therefore, there is a risk of drawing the wrong conclusion for some farmers, because they happen to have a sensor with not enough quality.

3. Propagating trust in risk assessment

In the previous section, we have provided examples of risks involved in risk management (related) systems. In this section we focus on the propagation of trust between the different

http://dx.doi.org/10.5772/intechopen.70741

parties that design, construct, manage and use these systems. Without the propagation of trust, it is impossible to assess risk using these systems, during construction as well as during its usage. The approach for propagation we describe is largely based on separation of concerns and will be discussed at the logical/functional level of abstraction, from an architectural point of view.

3.1. Separate concerns in risk assessment

A basic underlying problem for teams of multidisciplinary experts to vouch for a system as a whole is that they cannot do a proper review of the work of experts from another domain. They simply miss the expertise. For example, how can a mathematical analyst determine if measurements made by another expert can be trusted if he/she has no expertise in the field of making measurements? How can the analyst assess how much risk is involved in using these measurements? If they want to vouch for the system as a whole, they have to trust the other experts involved.

We state that it is important for continuous risk assessment of complex risk management (related) systems to separate the concerns for experts. This means that instead of assessing risk for a large monolithic system with lots of intertwined functional components, a conglomerate of components should be designed with risk management built in the components. Each expert can focus on their component which he or she understands. They connect their own components to others using well-defined interfaces. These interfaces take into account risk assessment issues, which we will be discussed later on. The idea of separation of concerns in distributed systems is sometimes also referred as 'unbundling'. Finding out where to 'draw the lines of separation' is beyond the scope of this chapter, as it is a topic of its own in distributed systems design. However, we can state that the following categorisation of types of expertise provides an indication of where to separate:

1. **Measurement.** For example, creating an accurate reflection of the physical reality often requires very specific know-how of sensors.
2. **Analysis and modelling.** For example, analysis and modelling require very specific mathematical expertise.
3. **Computation.** For example, parallelisation of computation requires specific knowledge of applied computational science.
4. **Presentation.** For example, letting people draw the right conclusion from information inside a computer requires specific knowledge of human-machine interfaces.

Once a design is separated into components that are understood by experts in their domain, the next step is to make information on risks that involved explicit. Experts should provide risk assessment-related information about the (un)certainty of the (delivery) of data/information of their component to other components explicitly. In this way it is possible to assess the risks involved of the system as a whole. Note that we do not consider the decomposition of a system into parts as something new: we use this as a stepping stone for the next sections.

3.2. Propagation of trust

Experts can provide risk assessment-related information about the output of their component, based on their knowledge of how the component transforms input into output. In order to do so, they also need risk assessment-related information with regard to the input of their component. If this is provided, it is possible to have (a certain level of) trust to propagate throughout the system, if components are designed, constructed and used according to the following rules:

1. Components determine if input is provided as promised. They establish a level of trustworthiness for each supplying component.
2. Components include risk assessment (related) information in their output. They provide information for establishing their trustworthiness to other components.
3. Components are auditable by third parties. Noninvolved experts can assess the risk involved in using a component.

In the next sections, we will describe the first two rules in more detail. If these rules are followed, the likelihood increases of being able to trace back potential root causes in case of incorrect behaviour. A more detailed description of the third rule is beyond the scope of this chapter as it involves auditing and certificate practices (**Figure 1)**.

3.2.1. Receiving as promised

Delivery of output as input to another component (e.g. measurement data, analysis results, model-based estimations of probability, etc.) has different aspects. For each of these aspects, risks can be identified. We provide a non-exhaustive list of aspects:

1. **Completeness.** Whether or not all input was received, having everything that is needed.
2. **Timeliness.** Whether or not all input example was received in time. Sometimes data becomes useless if it arrives too late. For example, receiving a warning about potential

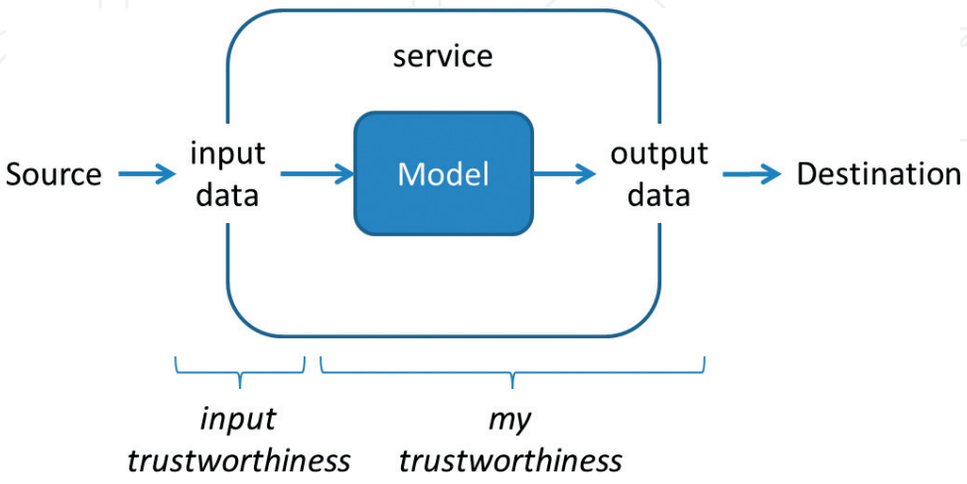

Figure 1. Basic trustworthiness model.

flooding 3 days after the flood is a problem for a system that provides information for people who have to decide on a possible evacuation. With respect to behaviour in time, the following types can be identified in terms of reliability (**Figure 2**):

i. **Perfect world**: input is always delivered on time.

ii. **Realistic OK**: sometimes, input arrives somewhat later than promised, but still in time to be useful.

iii. **Offline period**: sometimes, certain input is not delivered at all for a certain amount of time. After the period of silence, the input that should have been delivered during that time is not sent. This affects completeness.

iv. **Delay burst**: sometimes, bursts of input are delivered after the time it was useful to process. This does not affect completeness.

3. **Correctness**. The way in which input conforms to fact or truth. All the aspects of the correctness apply to both the arrival time and contents of the input. Aspects which play a role are:

4. **Accuracy and precision**: both aspects relate to the difference between the content of the input and the actual (physical) state of what the input pretends to provide information about (**Figure 3**). We define accuracy to be the size of the difference, whereas precision relates to the average difference between input and truth (e.g. a measurement and actual physical state).

5. **Consistency**: input (e.g. a set of measurements) is consistent if it is free of conflicts. For example, measurement data that shows that a normal household freezer would jump 20° C in 1 sec is not consistent. Note that a consistent set might be consistent and not accurate at the same time.

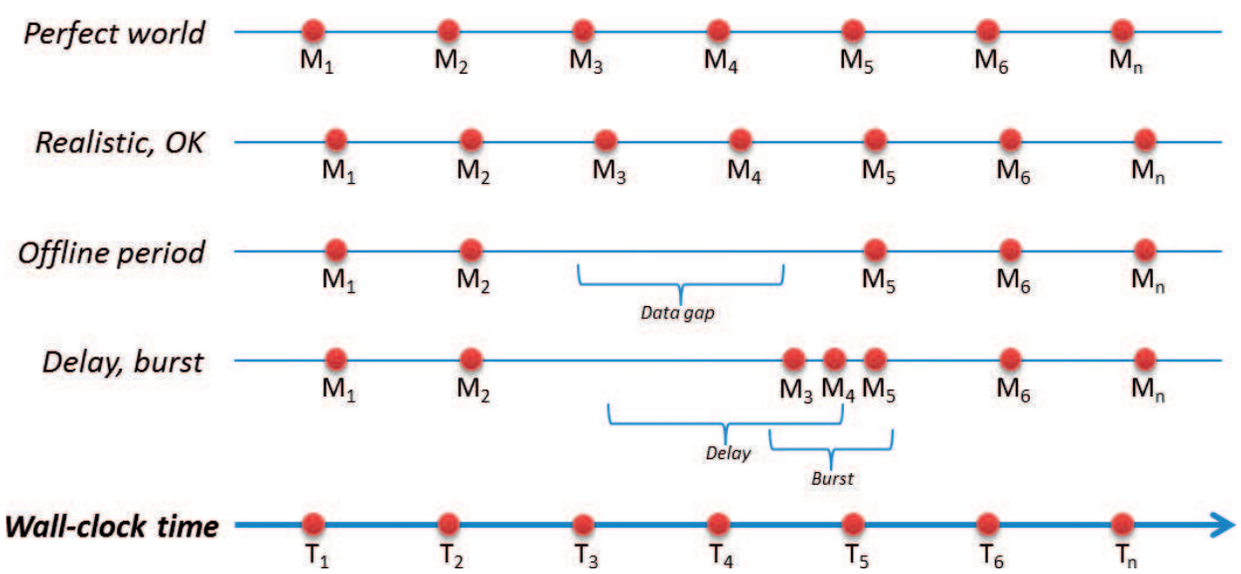

Figure 2. Aspects of timeliness. The display dots (M1-Mn) represent input data created at wall clock time T1-Tn.

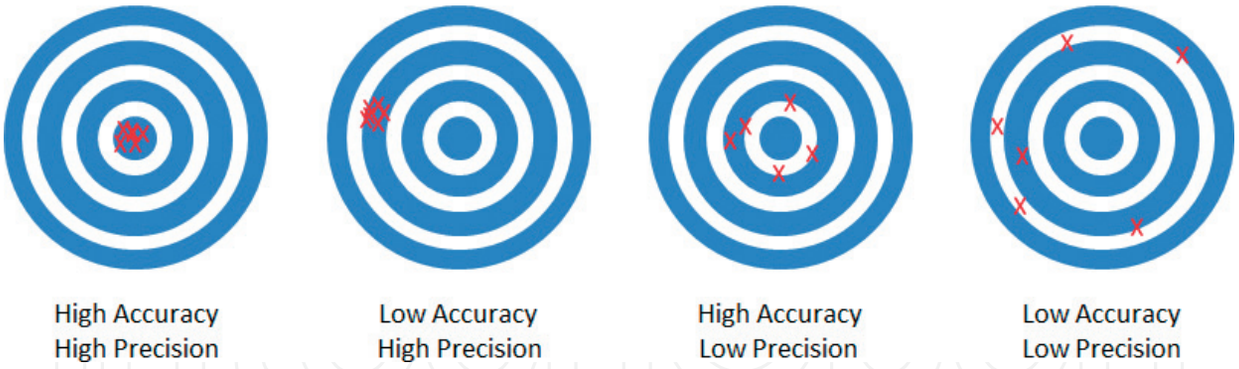

Figure 3. Relationship between precision and accuracy.

6. **Validity**: the degree to which input conforms to agreements on syntax and semantics. For example, if the temperature of a freezer is noted in degree Fahrenheit, it might be accurate, precise and consistent. However, if the agreement was to report in degree Celsius, the data is not valid.

Using the concepts of completeness, timeliness and correctness, we can define a tree of trustworthiness for a component as seen in **Figure 4**.

The trustworthiness of a component is determined by its availability to other components and the quality of the output it provides (in time). That quality can be described in terms of 'quality of transport' (QoT) and 'quality of data' (QoD), each from the viewpoint of completeness, timeliness and correctness. From a QoT perspective, the received input is considered as black box, and the focus is on the arrival in time. From a QoD perspective, the content, the data, is considered.

This tree of trustworthiness could also be used to design components that explicitly filter input based on the different aspects: timeliness, completeness and correctness (see **Figure 5)**. Depending on the impact of using input that, for example, did not arrive on time or was partially incomplete, a component might decide not to produce any output. This could in turn result into a cascade of components that stop producing output, thereby signalling the end-user that the system as a whole can no longer be trusted at the same level as before. Whether or not the system as a whole should show this kind of behaviour depends on the specific purpose

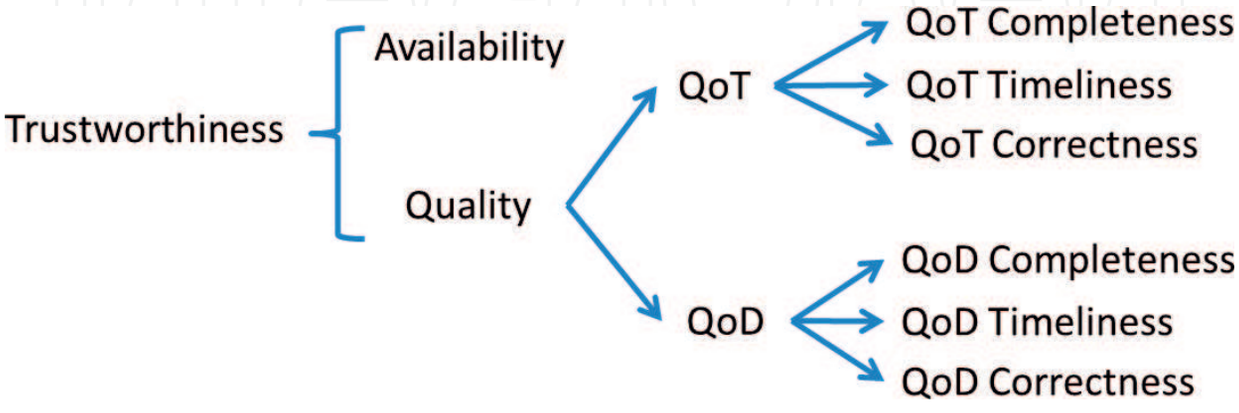

Figure 4. Tree of trustworthiness.

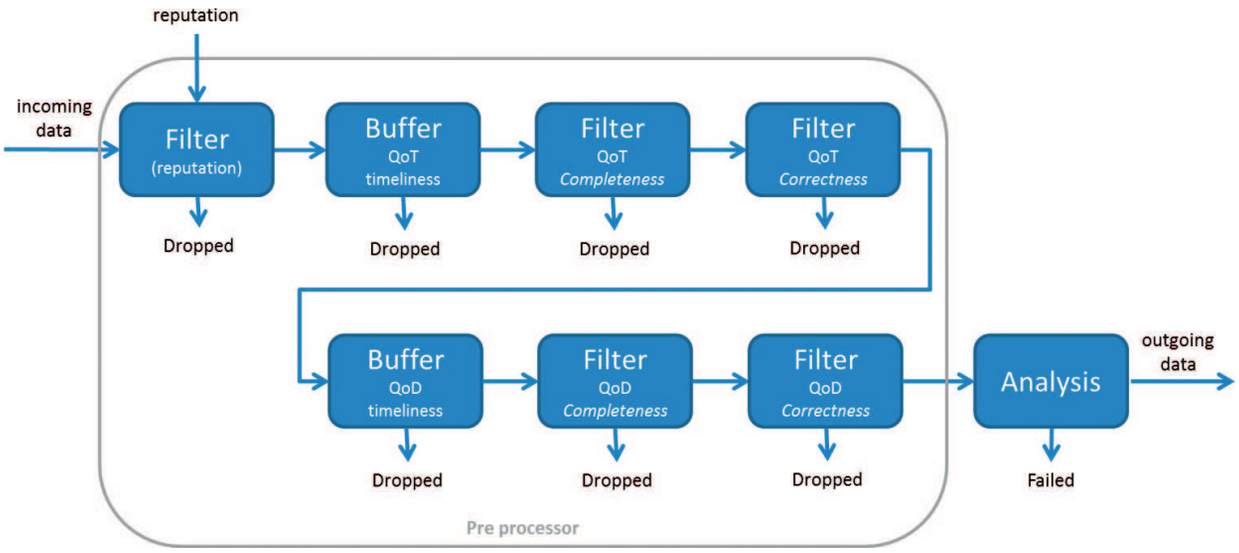

Figure 5. Filtering of input based on risk assessment-related aspects.

of the risk management system. It might also be possible to come up with 'best effort' output and explicitly communicate this with the output. This is covered in the next subsection.

3.2.2. Including risk assessment information for trust

In the previous subsection, we focussed on assessing risk by components that receive input. As described before experts from one domain of expertise cannot review the work of experts in another domain (they do not master). Therefore, components need to include information about the inputs that were used into their output. From a viewpoint of intercomponent communication, this can be done in two ways:

1. **In band**. When data/information is delivered to or retrieved by another component, information on the source and method for creating that data/information is included. This can result in a massive overhead of communication.
2. **Out of band**. Receiving components can ask a component for information about the source and method for specific data/information. This is less overhead in communication but poses more of a risk as this meta-risk assessment information is separated from the data/information that is communicated between components.

Wherever risk assessment information about produced data/information is made available (in band or out of band), there need to be agreements on the syntax and semantics of accuracy, probability, etc.

4. Conclusion

In this chapter we have discussed the concept of trust propagation in information and communication technology-based systems that are used for risk management, from a risk assessment point of view. We have provided examples of such risk management systems and shown

the possible types of risks involved. Furthermore, we have provided suggestions on how to enhance assessment of risk of these systems, by applying the concept of 'separation of concerns' and making risk assessment information explicitly available.

Author details

Kristian Helmholt*, Matthijs Vonder, Bram Van Der Waaij, Elena Lazovik and Niels Neumann

*Address all correspondence to: kristian.helmholt@tno.nl

Netherlands Organisation for Applied Scientific Research (TNO), The Hague, Netherlands

References

[1] Helmholt K, Courage W. Risk management in large scale underground infrastructures. In: 2013 IEEE International Systems Conference (SysCon); 2013. Orlando, Fl: IEEE; 2013. pp. 902-908. DOI: 10.1109/SysCon.2013.6549991

[2] van den Heuvel F, Schouten M, Abspoel L, Courage W, Kruse H, Langius E. InSAR for risk-based asset management of pipeline networks (poster). In: European Space Agency Living Planet Symposium; 9–13 May 2016. Prague; 2016

[3] de Bruijn R. et al. Differential subsidence and its effect on subsurface infrastructure: Predicting probability of pipeline failure (STOOP project). In: 19th EGU General Assembly, EGU2017; 23–28 April, 2017. Vienna, Austria; 2017. p. 15924

[4] Helmholt KA et al. A structured approach to increase situational awareness in low voltage distribution grids. In: 2015 IEEE Eindhoven PowerTech, Eindhoven; 2015. Eindhoven: IEEE; 2015. pp. 1-6. DOI: 10.1109/PTC.2015.7232779

[5] Helmholt KA, Broenink EG. Degrees of freedom in information sharing on a greener and smarter grid. In: ENERGY 2011: The First International Conference on Smart Grids, Green Communications and IT Energy-Aware Technologies; May 22–27, 2011. Venice, Italy; 2011

[6] van der Weerdt CA, Kort J, de Boer J, Paradies GL. Smart dairy farming in practice: Design requirements for user-friendly data based services. In: Conference Proceedings for the International Conference on Precision Dairy Farming. Leeuwarden, Netherlands; 21–23 June, 2016. 427-432

[7] Vonder MR, van der Waaij BD, Harmsma EJ, Donker G. Near real-time large scale (sensor) data provisioning for PLF. In: Guarino M, Berckmans D, editors. European Conference on Precision Livestock; 15 September 2015 through 18 September; 2015. pp. 290-297