OUTLINING COMPREHENSIVE SECURITY ANALYSIS OF A CRITICAL INFRASTRUCTURE NETWORK

T. TYRVÄINEN & I. KARANTA
VTT Technical Research Centre of Finland Ltd., Finland

ABSTRACT

This paper outlines a security assessment methodology for analysing critical infrastructure networks. The focus is on intentional attacks against critical infrastructure, but otherwise the scope is not delimited much. Comprehensive security analysis of a critical infrastructure network requires an assessment of the probability of an attack, the probability of success of the attack, the propagation of the consequences in the network and the severity of the consequences. In this paper, a critical infrastructure network should be understood as a network including different infrastructures, such as gas, water and electricity. The aim is that the interconnections between different infrastructures are built in the risk model. In the outlined methodology, the analysis starts with the identification of potential attackers and targets, and selection of analysis cases. Then, a network model is utilised to identify attack locations and assess consequences, and in the last steps, attack events and their probabilities are analysed. Although different steps of the methodology can use different risk analysis methods, they are linked so that dependencies between them can be taken into account, and total risk estimates can be determined. It is not specified which particular method should be used in each step, but some potential methods are discussed. The selection of methods can depend on the application target and the size of the problem.
Keywords: attacks, consequence analysis, critical infrastructure network, security analysis.

1 INTRODUCTION

A critical infrastructure is an asset that is essential to the functioning of a society or economy. Examples of critical infrastructures are electricity generation and distribution; gas and oil production, transport and distribution; water supply; telecommunications; agriculture, food production and distribution; financial services (e.g. banking); transportation (railway network, airfields etc.); emergency services (medical, fire and rescue); and security services (police and armed forces). A critical infrastructure network is any network (road network, telecommunications network etc.) used in the direct operation of any system on which critical infrastructures depend [1]. In this paper, a critical infrastructure network is understood as a network including different infrastructures, such as gas, water and electricity. The aim is that the interconnections between different infrastructures are built in the risk model.

Risk and security analysis of critical infrastructures [2,3] is considered challenging because a significant threat is not only an independent failure of the components, but also an intentional attack on the infrastructure. Analysis of potential attackers is difficult because they can vary a lot depending on the target and can have very different motivations, skills and goals. Incidents of attacks on critical infrastructure can also have many kinds of consequences that are difficult to measure. Critical infrastructure networks contain complex dependencies, and attack sequences are usually complex as well. This paper focuses on intentional attacks

WIT CONFERENCES
This paper is part of the Proceedings of the 10th International Conference on Risk Analysis (RISK 2016)
www.witconferences.com

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V6-N1-30-39

because they have potentially larger consequences than for example component failures, and public acceptance towards such risks is lower than towards other risks.

The risk assessment process is outlined on a general level in this paper. Although large networks are the main application target, it should also be possible to apply the same methodology to smaller networks or limit the analysis to chosen parts of a network. The analysis could be restricted to cyber security or it could cover all kinds of attacks against critical infrastructure. The methodology contains phases that use different methods. It is not defined which particular method should be used in each step, but some potential methods are discussed. The selection of methods can depend on the application target and the size of the problem.

A risk consists of probability and consequence. Therefore, to perform comprehensive risk analysis, both the probability of successful attacks and the consequences need to be determined. The probability of a successful attack comes from multiplyingthe probability that an attack is attempted by the probability that the attempted attack is successful. To determine the consequences, it needs to be determined which parts of the infrastructures the attack affects and what are the effects of the attack. Before these analyses are performed, it needs to be determined what kind of attacker could perform an attack and against which parts of the critical infrastructure. The analysis is comprehensive only if all significant attacker-target scenarios are considered.

Comprehensive risk analysis is resource-demanding work. Many types of information are required on different levels of detail. Attacker types, targets and ways of attacking need to be identified, and the structure of the network and potential consequences are also needed. Especially, modelling different attack scenarios can require very detailed data on the corresponding information systems and their vulnerabilities.

2 RISK ANALYSIS METHODOLOGY FOR CRITICAL INFRASTRUCTURE NETWORKS

Figure 1 illustrates different entities and variables of the problem and their dependencies. ‘Main target’ is the target that the attacker wants to attack. ‘Attack targets’ are the targets where the attacker aims the attack in order to cause harm to the main target. Two main areas that need to be modelled are the critical infrastructure network itself and the attacks leading to the failures of specific components of the network.

The analysis starts from the identification of potential attackers and targets. Attacker–target pairs are considered analysis cases, which are analysed step-by-step. The analysis proceeds deductively from the consequences to the origin of the attack. This approach enables to take into account dependencies between different analysis phases and to focus on high-consequence cases. The analysis includes six steps, which are discussed in the following subsections:

1. Identification of potential attackers and targets
2. Selection of analysis cases
3. Identification of attack locations in the network
4. Consequence assessment
5. Analysis of attacks
6. Analysis of the probability of an attack

Before the analyses, it is good practice to characterise the critical infrastructure network as well as its functions and components.

2.1 Attackers and targets

The components of the critical infrastructure network must be identified and gone through systematically. A component should be understood here as a wide entity, e.g. a power plant or gas distribution infrastructure. For each component, potential attackers must be identified. This requires characterisation of the functions and processes of the infrastructure component to understand its value for the company, public and critical infrastructure network on a reasonable level.

Attacker types should be as general as possible so that the number of analysis cases would be reasonable. Broad categories, such as hobbyist, government funded team, terrorist and competitor can be used.

Only those components that can be the main targets of attackers should be considered in this step. This excludes components which themselves are not important for the attacker but are needed by other important components.

2.2 Analysis cases

Analysis cases are attacker–target pairs identified in the previous step. The probabilities and consequences of analysis cases are tentatively assessed by expert judgement. Those cases which are considered risk-significant are taken into further investigation. Analysis cases can be prioritised for further analysis so that the presumably most important cases are analysed first.

2.3 Network model

In some cases, the attacker can achieve its goals in different ways. The attacker does not necessarily have to attack the main target directly, but can instead aim the attack against some other components of the network on which the main target depends. In other words, these other components can be other parts of the network that are critical with regard to the functioning of the main target. For example, a gas company may need communication services to be able to perform gas distribution.

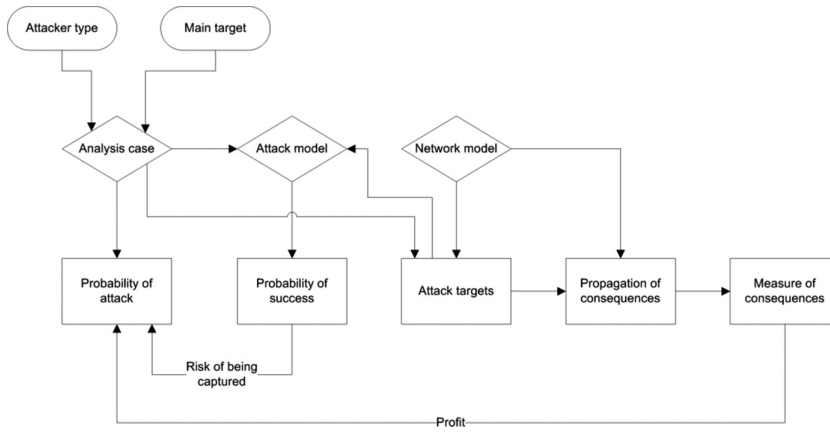

Figure 1: Entities and variables of the risk assessment problem.

The network should be modelled so that potential attack points could be identified from it and the propagation of consequences could be analysed. This requires extensive characterisation of the dependencies in the critical infrastructure network. The network model should preferably comprise all connected critical infrastructures.

The identification of attack targets corresponds to the identification of minimal cut sets [4], which are minimal failure combinations that cause the analysed top event, the goal of the attacker in this case. Minimal cut sets are best identified from fault tree analysis, but in an article by Apostolakis and Lemon [5], minimal cut sets of small critical infrastructure networks were identified. Here the aim is mainly to analyse wider networks with higher level of abstraction than in [5].

There are three main options to identify the potential attack points:

1. Simulation
2. Solving minimal cut sets analytically
3. Expert judgement

Options 1 and 2 would be beneficial because they can be automated. However, it should be possible to build accurate enough network models. One question is whether binary logic would be sufficient for the model or if multi-state logic would be needed. Binary logic would be computationally beneficial, and then, the approach from Apostolakis and Lemon [5] could be utilised. For multi-state modelling, dynamic flowgraph methodology (DFM) [6] would be an option. DFM also enables modelling of time-dependencies in the network, e.g. delays in transportation.

Another question is how probabilities of consequence propagation should be taken into account. An event might not lead to another certainly but with a probability smaller than 1. An attacker will not perform an attack if the desired consequences are very unlikely. Probabilities of consequence propagation must be considered in the consequence assessment but it might be sufficient to perform this step without them. An option would be to consider in this step only those connections of the network for which the propagation probabilities are large.

It should be possible to select any component of the network model for the analysis. Hence, the traditional fault tree approach [4] would not be the best option.

2.4 Consequences

Potential attack points were identified in the previous step. Now, the consequences need to be estimated for each attack point combination. The network model can be used in the propagation of the consequences in the network to take into account all the consequences of the attack. Measuring consequences is challenging because the consequences can be very different for different attacks and targets. Attacks can threaten human lives, important services, structures or information security, and in addition to direct consequences, there can be a wide range of indirect consequences.

The cascade diagram method introduced by Utne *et al*. [7] is a potential method for assessing the propagation of the consequences and for calculating total consequences. A cascade diagram starts with an initiating event which is a successful attack against a component of the critical infrastructure network or other harmful event. Each related component has a conditional failure probability, the extent of consequences caused by the unavailability of the component as well as the duration of the unavailability. The total

consequences are calculated from the diagram based on these values. It could be worth considering if this approach could directly be applied using the network model without constructing separate cascade diagrams.

Simulation is another option for analysing the propagation of consequences.

For analysing the magnitudes of consequences, a promising candidate is Bayesian networks [8]. They have been used, for instance, in the consequence analysis of maritime security threats, which contains similarities to the analysis of critical infrastructure security threats. Another option is to perform purely qualitative assessment by expert judgement. For economic consequences, the methods of cost estimation [9] may be used.

2.5 Attacks

It needs to be analysed how probable it is that an attack is successful. There can be many alternatives for performing the attack and the attack can be a complex event sequence involving many conditions. Hence, systematic and structured ways to model attacks are needed. Either qualitative or quantitative analysis could be used. It would be challenging to find data for quantitative assessment.

This step will likely require extensive system analysis to identify vulnerabilities and the effects of their exploitation. A complex system can be characterised by listing its critical functions, critical subsystems, failure modes and impacts of failures. Attacker types have to be also considered to identify potential attack styles, e.g. installing virus or denial-of-service attack.

Attack trees can model the sub-goals the attacker needs to achieve so that the attack is successful [10]. Information security has been the main application area of attack trees. Attack trees are usually analysed qualitatively, but they can also be analysed quantitatively in the manner of fault trees.

A possibility would be to perform game theoretic risk analysis [11]. An attack can be interpreted as a game between the attacker and security personnel. Game theory could be applied in combination with attack trees.

2.6 Probability of an attack

The probability (or frequency) of an attack can depend on the motivation, profit, the probability of success, the probability of being caught, and harm caused by being captured or identified. The profit depends a lot on the attacker. If the attacker is funded by an organisation or state, the profit made by the organisation or state should be considered. The consequences of successful attacks can be some sort of measure for profit, but not perfect.

Bayesian network is a suitable method for estimating the probability of an event affected by several variables [8]. It has been used, for instance, in the estimation of the probability of a terrorist attack in maritime domain. Another option is to perform purely qualitative assessment by expert judgement.

3 ILLUSTRATIVE CASE EXAMPLE

To provide something more concrete, the example of a progression analysis case is sketched in this chapter. This example is based on a gas distribution use case from Böttinger *et al*. [12]. Figure 2 presents a simple infrastructure network. COM1 and COM2 are communication providers, GAS1, GAS2 and GAS3 are gas companies and PLANT is a power plant.

The six steps of the analysis are taken through with one analysis case with brief descriptions.

3.1 Attackers and targets

Gas company, GAS2, is identified as a target. Other nodes are potential targets as well but GAS2 case is the focus here. A state-sponsored hacking group is identified as a potential attacker type against the gas company.

3.2 Analysis cases

An attack by a state-sponsored hacking group against the gas company is considered as a significant analysis case.

3.3 Network model

From the network (Fig. 2), it is identified that GAS2 depends on COM1, COM2, GAS1 and GAS3. Loss of each could cause loss of gas distribution from GAS2. Hence, GAS2, COM1, COM2, GAS1 and GAS3 are all potential attack targets to cause loss of gas distribution from GAS2. Here, the focus is on attack against COM1.

3.4 Consequences

Due to a successful attack against COM1, customer communications, partner communications, billing queries, metering services and pipeline access of GAS1 are shut down. Loss of communication can cause explosion and loss of gas supply because failsafe valves cannot be controlled. The gas supply of the country is lost if GAS2 is lost. Consequences could propagate to electricity supply of the country because PLANT needs gas from the gas

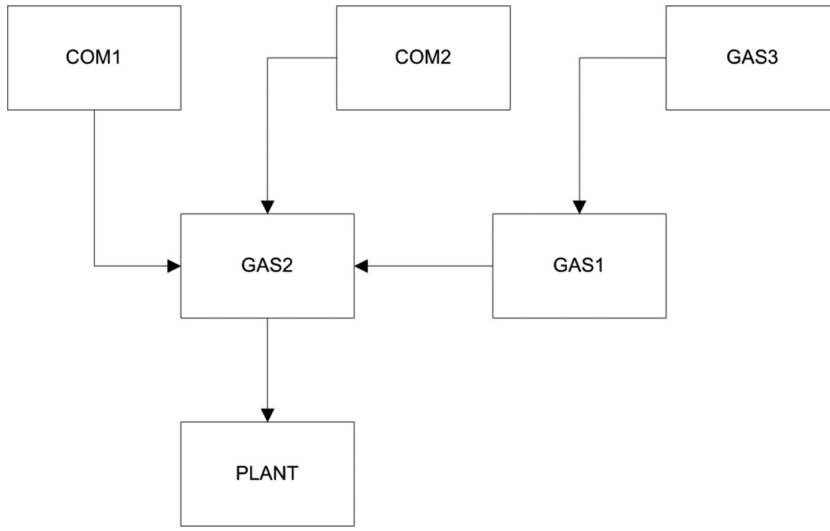

Figure 2: Infrastructure network related to gas distribution.

company. A significant part of the electricity supply of the country could be lost. In principle, attack against COM1 could also have wider consequences, but here it is assumed that the attack is focused only on the communication services of GAS1 because it is a much more likely scenario if GAS1 is the main target.

Figure 3 presents a simplified cascade diagram [7] for the attack. Variable *P* represents the conditional probability of the event given that the preceding event occurs. It is given as a number between 1 and 5. Value 5 means that the event occurs with certainty and value 1 represents the lowest probability. Variable *E* represents the extent of consequences and *D* the duration of the conditions. They are also measured on the scale between 1 and 5.

The expected consequence of the attack is (by formulas from Utne *et al*. [7])

$$C = 1 \cdot (10^3 \cdot 6^{2-1.5} + 10^{4-4.5} \cdot \left(10^5 \cdot 6^{3-1.5} + 10^{4-4.5} \cdot 10^4 \cdot 6^{2-1.5}\right) \approx 470000. \quad (1)$$

Even though there is no reference value, this number is clearly high.

3.5 Attacks

Figure 4 presents a simplified attack tree that contains sub-goals for reconnaissance, denial of service attack and staying anonymous. These three sub-goals need to be achieved so that the attack is successful. Denial of service can be achieved by three different types of

Figure 3: A cascade diagram for attack against COM1.

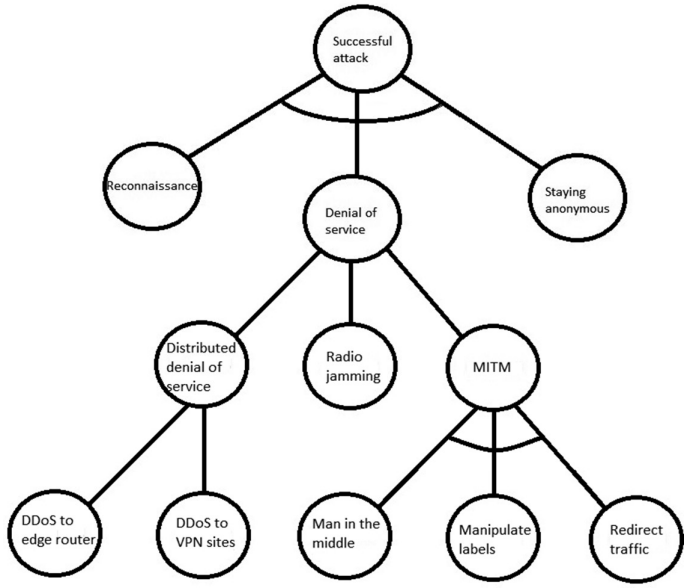

Figure 4: Attack tree for the attack against COM1.

attacks: distributed denial of service, radio jamming or man in the middle attack. The tree could be developed further by adding more detailed sub-goals or new ways of attack. The probability of success is assessed to be low.

3.6 Probability of an attack

The state of the hacking group receives moderate benefits from the loss of energy supply of the country. However, the probability of success is assessed to be low, and the risk of being detected medium. The probability of the attack is assessed to be low.

The total result is that consequences are high, but the probability of such an event is low.

4 SIMULTANEOUS ATTACKS

Most dangerous attack scenarios are those where multiple attacks are performed simultaneously. Attackers know this, and therefore, the likelihood of such attacks is significant and needs to be taken into account in the risk analysis. In the methodology outlined in this paper, this means that analysis cases with multiple main targets must be constructed. A problem is that this can increase the number of analysis cases significantly. It could be sensible to consider only such multiple target cases where the attack scenarios are significantly dependent with regard to consequences or probability.

When multiple attack scenarios have been identified, they can be analysed as single attack scenarios. They may be identified in the following way. First, go through the list of individual attacks. For each attack, consider all other attacks that might be combined with it; these can be identified by considering 1) whether the two attacks have been used together in past successful attacks; 2) is there a dependence between the attacks, e.g. the success of attack 1 enables the easy implementation of attack 2; 3) are there synergies between the attacks, e.g. the use of attack 1 multiplies the effects of attack 2. For each attack pair thus formed, consider if other schemes would complement the two by the abovementioned criteria.

5 DISCUSSION

Analysing a large critical infrastructure network is very resource demanding and the risk model can grow to be very large. It is a challenge to choose methods that are efficient enough. The model and methods have to be kept as simple as reasonable but accurate enough for meaningful risk analysis. Too detailed modelling of the network should be avoided. Possibilities to model multiple ‘components’ and relatively large entities by a single node should be considered. It would be beneficial if as much of the analysis as possible could be automated. It should be possible to use the same network model for all analysis cases. It would be a remarkable asset if the network model could be utilised for automatic consequence assessment.

Critical infrastructure typically has multiple failure modes. Loss of the whole infrastructure is usually the most important with regard to risk analysis, but an infrastructure could also have different functions that can fail separately. There are several ways to account different failure modes in the methodology, including the following:

1. Different failure modes are separated completely in the network model and analysis cases.
2. One component is used for multiple failure modes in the network model, but different analysis cases are constructed for different failure modes.
3. One multi-state component is used for multiple failure modes in the network model and different failure modes have separate analysis cases.

4. One component and common analysis cases are used for multiple failure modes and they are separated only in the consequence and attack analyses.

The best option can depend on the scope of the analysis. It is recommended to screen out failure modes with small consequences and to make simplifications where possible, e.g. merging failure modes.

It could be possible to simplify the analysis if the identification of attack locations was left out, and instead, attacks against each component of the network were simply analysed for probability and consequences one by one. This would be more straightforward, but some details could also be missed. Not all indirect attacks might be accounted for properly, i.e. if an attacker attacks against some other component to cause the loss of the main target. Because of indirect attacks, it is important to consider what kind of attacks could cause the loss of a specific component. This analysis can however be difficult and laborious to perform.

An important application of the risk model would be to analyse the effectiveness of countermeasures. This analysis could be performed so that for each countermeasure, the model is changed so that the effect is taken into account, and the change in total risk is measured. However, this could be very time-consuming. Some intelligent and efficient way to perform this analysis should be found.

Measuring the risk importances of components is an essential part of the risk analysis of complex systems. Based on this, improvements and maintenance activities can be prioritised effectively. Risk importance measures are well-studied in the risk assessment of nuclear power plants, but they require quantitative approach and cannot necessarily be directly applied in this domain. Especially, if a qualitative approach is used, determining risk importances should be considered carefully. Some other forms of sensitivity analysis should also be considered.

It would be valuable to perform uncertainty and sensitivity analyses for the model because uncertainties in variable values are large in many cases. This could however be computationally too time-consuming. It could be realistic to perform sensitivity analysis just for a limited set of variables instead of comprehensive uncertainty analyses and sensitivity analyses. Quantitative uncertainty analysis would be more straightforward than qualitative.

A challenge is that critical infrastructure and potential attackers evolve in time. The results of the risk analysis can change significantly. Hence, the risk model should be maintained and updated continuously. Construction of such a risk model that is easy to update would therefore be very beneficial.

6 CONCLUSIONS

This paper outlines a methodology for the risk analysis of critical infrastructure networks. Both the probability and consequences of a successful attack are analysed. In the methodology, analysis cases are determined first. Then, the consequences are analysed, and finally, the probability of an attack is assessed. This order enables to take into account dependencies between analysis phases, such as the probability of the attack depending on the expected consequences. It is possible to aim the focus on the most significant cases and cut out less important cases before detailed analysis.

The methodology is sketched on a very general level, and the choice of the actual analysis methods has not been made. Use of both qualitative and quantitative methods is possible. Some potential methods are suggested. The choice of methods can be made based on the

scope of the analysis. However, establishing standard analysis procedures would be beneficial so that the same tools could be applied in many critical infrastructure analyses.

REFERENCES

[1] Knapp, E., *Industrial Network Security – Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Syngress: Waltham, 2011.

[2] Hokstad, P., Utne, I. & Vatn, J., *Risk and Interdependencies in Critical Infrastructure: A Guideline for Analysis*, Springer Series in Reliability Engineering: London, 2012.

[3] Lewis, J.A., *Cybersecurity and Critical Infrastructure Protection*, Center for Strategic and International Studies: Washington D.C., 2006. http://dx.doi.org/10.1002/0471789542

[4] Vesely, W.E., Goldberg, F.F., Roberts, N.H. & Haasl D.F., *Fault Tree Handbook*, U.S. Nuclear Regulatory Commission: Washington D.C., 1981.

[5] Apostolakis, G.E. & Lemon, D.M., A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, **25**(2), pp. 361–376, 2005.

[6] Garrett, C.J., Guarro, S.B. & Apostolakis, G.E., The dynamic flowgraph methodology for assessing the dependability of embedded software systems. *IEEE Transactions on Systems, Man and Cybernetics*, **25**, pp. 824–840, 1995. http://dx.doi.org/10.1109/21.376495

[7] Utne, I.B., Hokstad, P. & Vatn, J., A method for risk modelling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety*, **96**, pp. 671–678, 2011. http://dx.doi.org/10.1016/j.ress.2010.12.006

[8] Roventa, E. & Spircu, T., Bayesian (belief) networks (Chapter 5). *Management of Knowledge Imperfection in Building Imperfect Systems*, eds. E. Roventa & T. Spircu, Springer-Verlag: Berlin, pp. 133–152, 2009.

[9] Mislick, G. & Nussbaum, D., *Cost Estimation – Methods and Tools*, John Wiley & Sons: Hoboken, 2015. http://dx.doi.org/10.1002/9781118802342

[10] Schneier, B., *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons: New York, 2000.

[11] Bier, V.M. & Azaiez, M.N., *Game Theoretic Risk Analysis of Security Threats*, Springer: New York, 2009.

[12] Böttinger, K. et al, Use case scenario report, ECOSSIAN: European control system security incident analysis network, 2015.