National Protective Security Authority

CAE:

SECURITY-INFORMED HAZOP

CONTENTS

FIGURES

TABLES

01. INTRODUCTION

A hazard and operability study (Hazop) [1] is an effective technique for the identification and analysis of hazards and operational concerns of a system. It has been developed in the chemical industry and became a key tool in carrying out safety analysis in a variety of industries, including nuclear and railway.

The central activity of a Hazop is to identify the hazards posed to a system not on the physical system itself, but on a representation of it. The design representation shows the system at more or less detailed level in a symbolic form. It has, in principle, no restriction on the form as long as it is clearly documented and understandable by all the team, of which the skills should be complementary. The investigation is then based on this representation and progresses methodically under the control of the study leader.

The growing need to provide security and safety assurance led to the development of a security-informed Hazop, which is a variation to a conventional Hazop to address security issues. It provides an opportunity for a structured and informed discussion about the security risks associated with a system.

[1] IEC61882:2002 Hazard and operability studies (HAZOP studies) - Application Guide, 2002

02.
SIGNPOSTING

This is the third detailed generic guide in the stack of resources for security-informed safety assurance. Figure 1 below shows its location in the set of guides (highlighted in red).

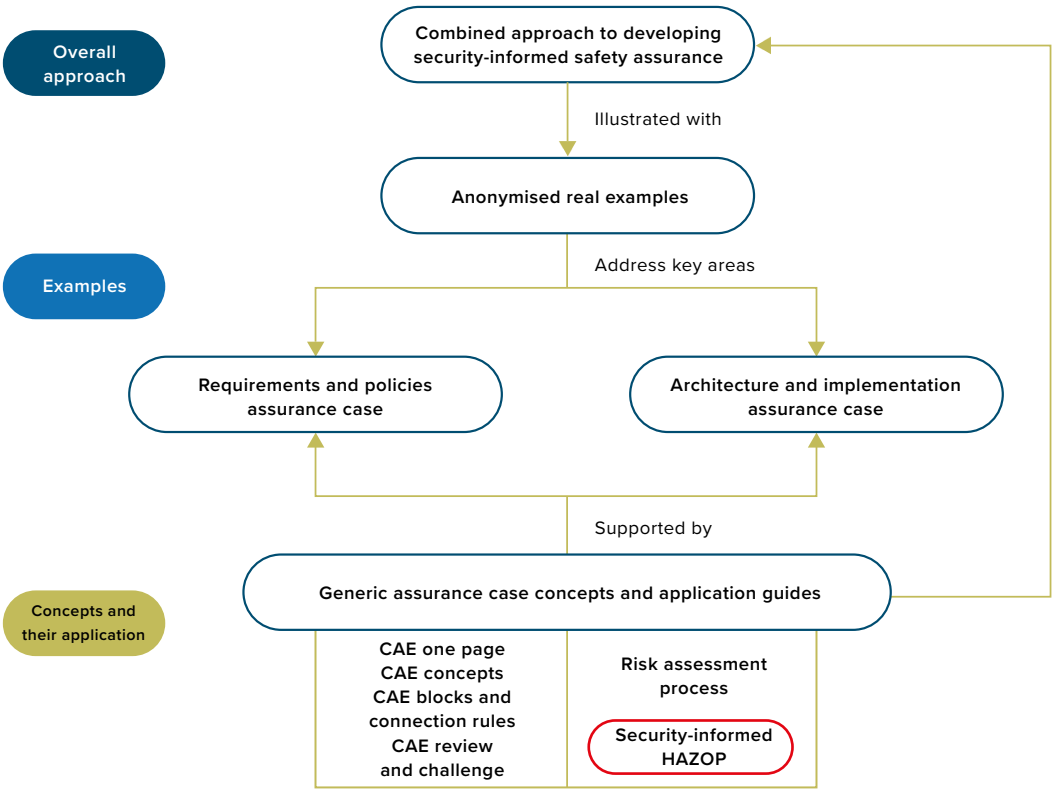

Figure 1: Location of this guide in the set of resources

03. GUIDANCE

3.1 PLANNING THE STUDY

A Hazop can be a lengthy process that needs to be planned in advance and both project and operational plans have to be in place. The main planning considerations are:

- ensuring the availability of the design representation and identifying the properties that should be examined;
- identifying and briefing the team members; and
- selecting a set of guide words (which expresses and defines a specific type of deviation from design intent) for use during the study and providing the interpretation when they are applied.

In order to outline the approach, a Hazop note is produced prior to the meeting and distributed among the team. It explains the methodology used and informs about the design representation that will be used at the workshop.

In a conventional Hazop study, the guidewords relate to the data flow and the data value between the links (see Section 3.5). For a security-informed Hazop a set of guidewords is still required with comparable failure modes, but the causes are security-related. In the security-informed case, the STRIDE keywords (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) [2] can be used as a basis for potential causes. The main attacks are:

- **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorised changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- **Denial of service**. Denial of service (DoS) attacks deny service to valid users – for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

These can then be linked to the guidewords, as they provide means for implementing attacks such as spoofing and tampering (see Table 1).

Guideword	Possible Interpretation	Possible causes
No	No message sent	Denial of service
Invalid	Illegal format	Spoof / tamper
Wrong	Wrong data value	Spoof / tamper
Inconsistent	Mismatch between data sets	Spoof / tamper / substitution
As well as	Additional message	Spoof / tamper / replay
Other than	Wrong message type, source, destination	Spoof / tamper
Part of	Element of message missing	Spoof / tamper

Table 1: Example guidewords, interpretations and security-related causes

The Hazop analysis applies these guidewords systematically to each component interface, including interfaces at the system boundary.

[2] I Microsoft. The STRIDE Threat Model. URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

3.2 HOLDING THE MEETING

At the start of the meeting the purpose of the study and design representation that was distributed before the meeting are reviewed and if necessary, updated. In this way it is ensured that the entire team understands the system and the particular type of representation to be studied.

Following the introduction, each link or component of the design representation is examined applying the provided guide words to them in order to identify hazards and their causes and consequences in accordance with the defined scope and objectives of the study. The method is to investigate what deviations could occur in the values from their design intent, what could cause the deviations, and what effects this could have.

The guide words, each of which focuses on a particular type of possible deviation, may have different interpretations depending on the character of the connection. This makes their careful selection in the planning process and their interpretation in the given context an important step. For each attribute of the individual entity it has to be decided whether the guide words are meaningful. If the answer is yes, the possible causes and consequences of the deviation are enquired. In this way, hazards and consequences are identified.

A sample Hazop worksheet is shown in Table 2 below.

ID	Interface	Guide word	Interpretation	Cause(s)	...
1	In1	No	No signal	Jammer	

...	Immediate effect	Indication/ Protection	Hazard failure	Question/ Recomm,	Answer/ Comment
	Loss of real time status	Internal timeout System to fail-safe mode	Loss of service	Transmit two frequencies	

Table 2: Sample Hazop worksheet

The meeting ends with the documentation of the activities of the study. The documentation should be agreed by the team and captured in a summary report.

3.3 DEALING WITH THE FOLLOW-UP AND CONCLUDING THE STUDY

The follow-up of the Hazop generally deals with uncertainties, which must be resolved before the study can be concluded. If questions are raised during the meeting, it may be necessary to add a further discussion or convert each outstanding question into a recommendation for further study in order to achieve a thorough examination of the design representation. In the end the Hazop must have identified:

- any hazards
- recommendations to mitigate the identified hazards

A summary report is produced to record any hazardous system failures identified (see Table 3 as an example).

Ref	Hazardous Failure
H1	Loss of service
H2	...

Table 3: Hazard list example

The report should also summarise the recommendations to prevent service failures (see Table 4).

Ref	Recommendation
H1	Transmit on two frequencies
H2	...

Table 4: Recommendation summary example

The potential attacks and associated hazardous failures should also be summarised. The capability level required to implement each attack should be identified. Attacks that require a lower capability than the target level defined in the risk assessment configuration step should be highlighted.

Ref	Hazardous Failure	Scope	Capability	Hazard Failure	Recommendations
A1	DoS attack on interfacing network	All services affected	C	H1: Hazardous system failure, H2: ...	R1
A2	...				

Table 5: Attack summary

3.4 PENETRATION TESTING

The results of the security-informed Hazop are used to guide the penetration testing of the system (if this is possible). In these tests the system vulnerability is tested by attacking it using various forms of scenarios in order to prove the robustness. The results and potential weaknesses of the tests feed back into the hazard analysis and the assessment of the credibility of attacks for the attacker capability of concern.

3.5 GUIDEWORDS

3.6 CONVENTIONAL HAZOP

Conventional guidewords relate to the data flow/data value between links.

Data flow	No Action
Data flow	Faster / slower
Data flow	Part of Action
Data flow	As well as / other than
Data flow	Wrong source / destination
Data flow	Early / Late Action
Data value	Wrong Value
Data value	Invalid Value
Data value	Incompatible Value

3.7 SECURITY-INFORMED HAZOP

For a security-informed Hazop study the guidewords can be interpreted with the following possible causes of failure modes.

No data flow	Denial of service attack Tampering – interference Tampering – equipment Tampering – software/data
Faster / slower flow	Tampering – Interference
Part of intended flow	Tampering – software/data
As well as intended flow	Spoof message injected (compromised source) (compromised link)
Other than intended flow	Tampering – networking + stolen authentication
Wrong source / destination	Tampering – man in the middle + stolen authentication
Stale value	Denial of service attack Compromised source (repeat send) Replay attack
Wrong but valid value	Compromised source Replay attack (link) Spoofing (stolen authentication + valid command)
Invalid value	Buffer overflow attack (could sabotage software)
Incompatible value(s)	Tampering with software/data

04.
ACKNOWLEDGEMENTS

This document is based on material developed in earlier projects partially funded by the UK Control and Instrumentation Nuclear Industry Forum (CINIF) and guidance from previous NPSA projects and published research by Adelard.

Disclaimer

This guide has been prepared by NPSA and is intended to support the implementation of security-informed safety assurance and the Claims, Arguments and Evidence (CAE) methodology. This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness.

To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the [report]. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

No Endorsement

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by NPSA. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI
Centre for the Protection of National Infrastructure