Technological Harm Identification Utilising

HCI HAZOP

Human-Focused for Socio-Technical Systems

v2.0 May 2021

Supporting guidance for the HCI HAZOP method

IN – Introduction

Team

The HCI HAZOP method is based around four main steps (1-4), described on subsequent pages as follows:

0	Prerequisites		
1	Definition	1a	Assessment scope
		1b	Objectives
		1c	Harm perspective
		1d	Participants
2	Preparation	2a	Plan study
		2b	Collection
		2c	Element lists
		2d	Item granularity
GW	Guide words		

Draft guidance

This guide is work in progress. It includes instructions, tips, guidance and materials being built up as HCI HAZOP is applied to various socio-technical systems. Check back to this data repository for future updates. For further background, please read the paper:

> Colin Watson and Ahmed Kharrufa, 2021, *HCI - H is also for Hazard: Using HAZOP to Identify Undesirable Consequences in Socio-Technical Systems*, ACM COMPASS 2021
> https://doi.org/10.1145/3460112.3471959

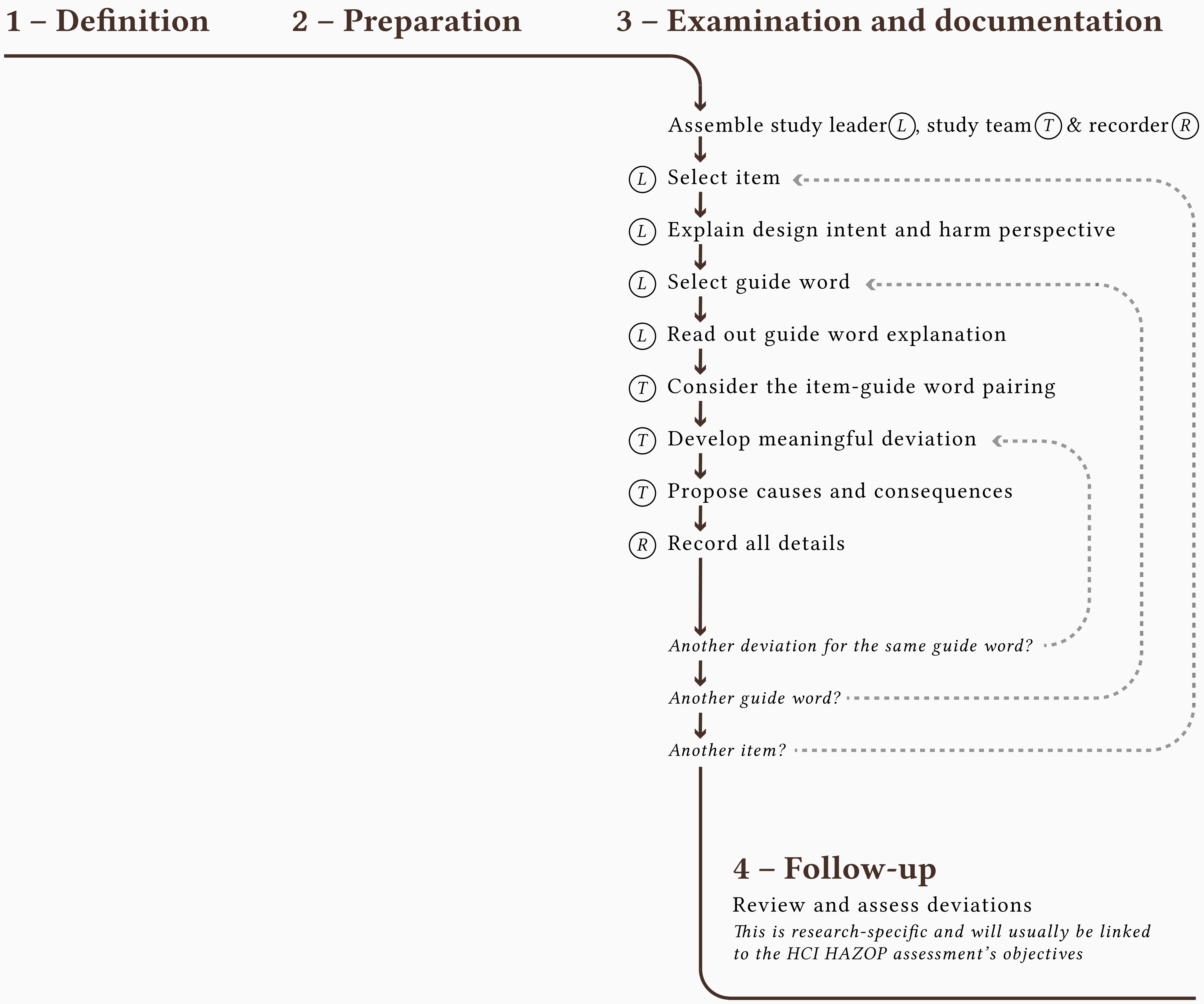
Also consider reading the international standard for the more generic HAZOP process:

> International Electrotechnical Commission, 2016, *IEC 61882:2016 Hazard and operability studies (HAZOP studies) - Application guide*

Recent changes

v2.0	Inclusion of all materials from the two Pilot Studies described in the ACM COMPASS 2021 paper	May 2021

OD – Overview Diagram



1 – Definition

2 – Preparation

3 – Examination and documentation

Assemble study leader Ⓛ, study team Ⓣ & recorder Ⓡ

Ⓛ Select item

Ⓛ Explain design intent and harm perspective

Ⓛ Select guide word

Ⓛ Read out guide word explanation

Ⓣ Consider the item-guide word pairing

Ⓣ Develop meaningful deviation

Ⓣ Propose causes and consequences

Ⓡ Record all details

Another deviation for the same guide word?

Another guide word?

Another item?

4 – Follow-up

Review and assess deviations

This is research-specific and will usually be linked to the HCI HAZOP assessment's objectives

0 – Prerequisites

Team

The choice of Study Leader and Study Team is an important factor in the success of the method (see 1d). All those involved should have some prior training and awareness of the method. The Study Leader should be experienced in applying the method if possible, and members of the study team should be familiarised with the method and terms like *intent* and *deviation* in advance. HCI HAZOP-specific training materials are being prepared to assist with this.

The Study Team should be familiar with the system being assessed.

System

The HCI HAZOP method focuses on what can go wrong to cause detrimental effects on people in some part of defined socio-technical system. The system may well be something greater than the assessment scope (see 1a), but it is useful to have in mind the wider system. The system does not have be fully defined (e.g. early prototype) but this means there will be more ambiguity in how it works, which can be both good and bad. Ambiguity leaves more to participants imaginations, allows a wider exploration of possibilities and leads to fewer constraints. If a specific design is being assessed, greater definition is likely to be required. These are linked to the objectives of the study (see 1b).

The system and part(s) being assessed need to be defined and should clearly identify the design intent (desired or specified behaviours) for each element/step. This could comprise one or more of the following:

- Schematic diagrams
- Specifications
- Personas, walkthroughs, scenarios, sketches, storyboards, user journey maps and other descriptions
- Other textual and/or graphical descriptions
- Prototypes, wireframes and mock-ups.

Ensure whatever information is used to document the system is available and understandable to all participants (1d). If the assessment relates to an existing system, it will be important to ensure that is thoroughly and accurately documented, including any changes that have been made. For proposed changes/interventions, a complete definition may not be available or possible, leading to more speculative exploration of deviations.

It is possible to provide too much information to the Study Team, to the detriment of the assessment. Materials should be sufficient to document the system being assessed and provide sufficient detail so that the objectives can potentially be met.

1a – Assessment scope

Context

The wider system and its environment need to be understood by the Study Leader and Study Team since these have a baring on how deviations might occur. For example, a person's friends and family may have an influence of what they do, or provide informal input such as help and advice. Similarly, laws, regulations and related sanctions may alter behaviour in different ways.

System elements

The unit of assessment for a socio-technical systems can be considered an activity mediated by tools. Consequently, these notes use Activity Theory as a lens to look at these things and to help define the scope by considering the unit of analysis for HCI HAZOP as an activity. In this view:

- The actors doing the activity (the person or people doing the activity and actions - the subject)
- The community and everyone else involved
- Their roles (division of labour)
- The rules and norms within that activity structure
- The outcomes (people's meaningful goals).

Activity Theory is a hierarchy of objects in which an activity is linked to a motive, an action to a goal, and an operation to a condition.

Scope

The scope of an individual assessment session is often only parts of the system hierarchy (defined elements and boundaries). It may be that multiple sessions are planned, each dealing with different parts/stages of the system under consideration. If the scope is too large, it is likely there will not be enough time to explore the deviations, possible causes and consequences adequately. The objective of the assessment (1b) will also influence the scope. Factors which add to complexity of assessment, and thus duration are:

- Greater number of tasks/activities (additional deviations for each interaction/steps)
- Greater number of actors (additional interactions and motivations)
- Wider boundaries/environment (inclusion of additional actors, mediating tools and other artifacts)
- Greater definition of all the elements (additional deviations around every specified detail)
- Lesser or contradictory definition (where there is insufficient detail leading to greater speculation)
- Systems that span longer time periods (additional sequencing/timing deviations)
- More possibilities for occurrence of harms (additional deviations).

In practice, it is best to begin with a smaller scope and explore this extensively without being rushed. If it seems the assessment scope is too large, consider stopping the session in the allocated time and resume again later after a break. A preliminary session may provide a feel for how much can be covered within a 1-2 hour session given the type of system and its definition.

1b – Objectives

Deviation coverage

Given the nature of socio-technical systems, and the many potential actors with their own motivations who can influence activities and actions, it is unlikely that all possible deviations can practically be enumerated (this can be the objective of a more conventional HAZOP in which the system could be more constrained). This means the HCI HAZOP assessment's objectives should state whether the assessment is time-limited or continues until deviation identification is exhausted.

Some assessments may be reviewing or building upon previous ones.

Scoping

An assessment may want to focus on particular actors, activities and actions within a socio-technical system. In this case the boundaries and interfaces need to be clearly defined and also whether activities in the past/future need to be assessed.

Harms

There is an implicit assumption that the harm perspective considers what harms might occur to the primary human actors (1c), but could be something else, including just some of the actors. This needs to be confirmed in the objectives.

Purposes

The objectives also need to state what the deviations identified will be used for. For example, as inputs to a human-focused risk assessment, to contribute to the design process, to identify mitigations.

1c – Harm perspective

Primary actors

For HCI HAZOP the perspective to consider harm impacts is from the primary human actors' point of view. Harms can be financial, physical, mental, and emotional including stress, fatigue, distraction and demotivation.

Other perspectives

Other perspectives are possible, such as from the point of view of the owner of the technical system, or assets like the technical system itself, but these are not usually the focus of HCI HAZOP.

1d – Participants

Study leader

The study leader is responsible for the defining (step 1), preparations (2), facilitating the assessment and ensuring the results are recorded (3) and that the assessment's objectives are met (4). They will typically be very familiar with undertaking HCI HAZOP assessments through training and experience, have good knowledge of the system, but not be related to the particular design/project and be independent from and to anyone in the study team, and have no conflict of interest in the outcomes of the assessment.

During the assessment, the study lead is responsible for selecting each item, explaining the design intent, reminding the team of the harm perspective and then reading out and explaining each guide word in turn. They will ensure the assessment is systematic and that the discussion does not stray from identification of deviations to intents - for example, some team members may raise consequences or causes instead of first identifying a deviation.

Study team

The assessment team should comprise designers, those who will use the system, those who will maintain the system and relevant specialists as necessary. They ought to be very familiar with any parts of the system that already exists and of the design of any proposed changes.

Recorder

The recorder does not take part in the identification of deviations, possible causes and consequences, but instead documents these aspects as they are identified, discussed and confirmed by the study team.

2a – Plan study

Information and data

Identify all the information and data requirements.

Design materials

Identify the necessary design materials for the required scope and objectives.

Meeting plan and bookings

Estimate the number of sessions needed to complete the assessment - this might be just one for a narrow scope and targetted objectives, but could be many. Availability of all participants for the full assessment, whether it is a single event or multiple sessions, is a priority.

Record keeping methods

Identify the method for documenting deviations during the assessment and how these need to be recorded to meet the objectives.

2b – Collection

Source information

Gather together in advance of the study:

- System definition (0)
- Scope of assessment (1a)
- Objectives (1b)
- Harm perspective (1c)

These will be used in 2c, 2d and the assessment itself.

2c – Element lists

Elements

By considering the unit of analysis for HCI HAZOP as an activity, the types of elements of relevance are:

- The actors doing the activity (the person or people doing the activity and actions - the subject)
- The community and everyone else involved
- Their roles (division of labour)
- The rules and norms within that activity structure
- The outcomes (people's meaningful goals).

Try to list out in advance every member of each of these element types.

Actors and others

The most important of these are the first two: various actors, and other individuals and groups. Apart from named individuals/roles that might be identified explicitly in the system's definition, include implicit ones too, and consider including:

- Their partners, friends, family and neighbours
- Other people in a similar role/situation to the main actors
- Local community groups
- Sources of support and information (e.g. government information, charities, voluntary groups)
- Civil servants
- Local/national government
- Society
- People who might have malicious intent (e.g. fraudsters, hackers, thieves).

Outcomes

List the expected motives and goals of the various actors and others by thinking about each person's/role's needs.

2d – Item granularity

Items

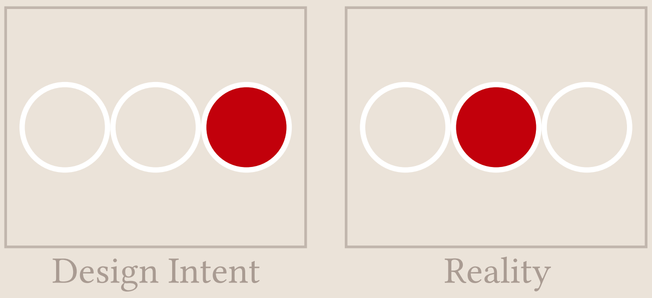
Once the scope is defined (1a), it is necessary to decide what type and granularity of elements (2c) are examined through systematically applying to them each of the guide words (G1-G3) in turn. The choice will depend primarily on the objectives (1b) and assessment scope (1a), but might typically be activities or possibly actions. In some cases it might be higher-level goals of one or more actors. For narrowly-scoped assessments, there might be a single action and therefore a single pass through the guide words applied to this, but in practice even a single action provides much opportunity for consideration of different actors' motivations and goals, and how the related technology is used and misused.

List

Usually there will be multiple items for each assessment, so these should be listed out in advance of the assessment.

Design intention occurs but ahead
or behind by sequence/order

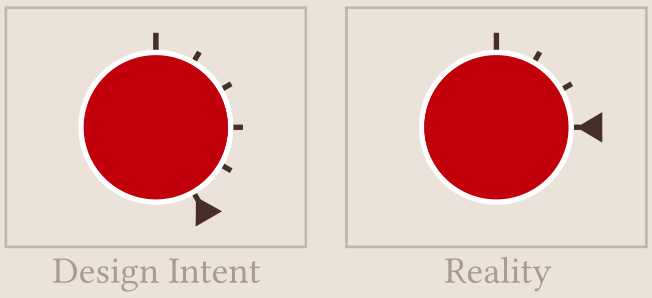
Order



Wrong order/sequence before or after intended, leading to some deviations (which cause negative consequences to people).

Design intention occurs but ahead
or behind by clock time

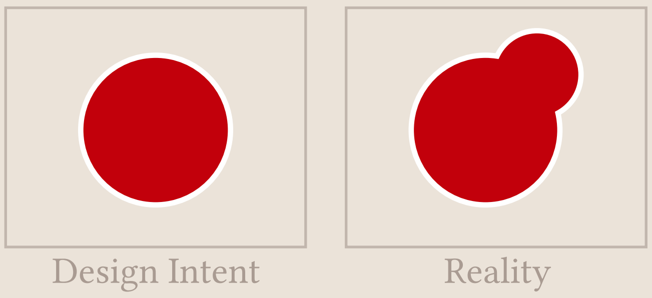
Time



Sooner/earlier or behind/later relative to intended time, leading to some deviations (which cause negative consequences to people).

All the design intent is achieved,
but also some qualitative increase

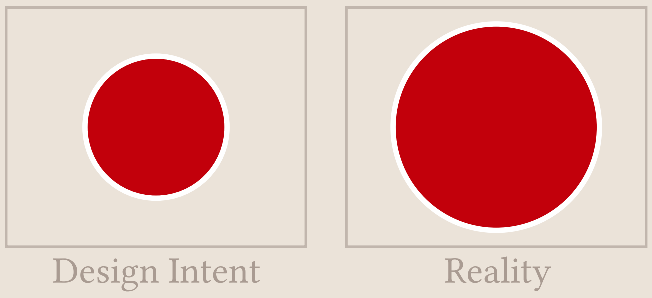
As Well As



Something else in addition to the intent, qualitatively. Think about what system deviations (which cause negative consequences to people) might lead to other outcomes as well.

All the design intent is achieved,
but also some quantitative increase

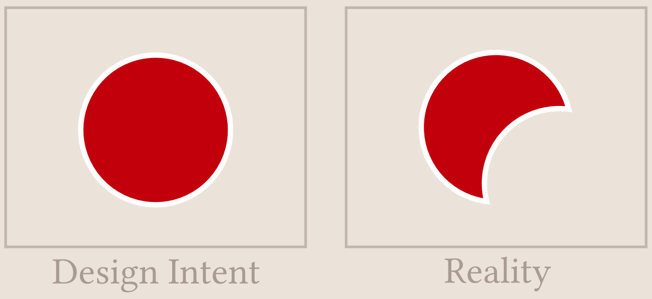
More



More of the intent, measured quantitatively (such as count, rate, size, position, duration, other measurable variable). Think about what system deviations (which cause negative consequences to people) might lead to measurable increases numerically.

Only part of the design intent is achieved
by some qualitative decrease

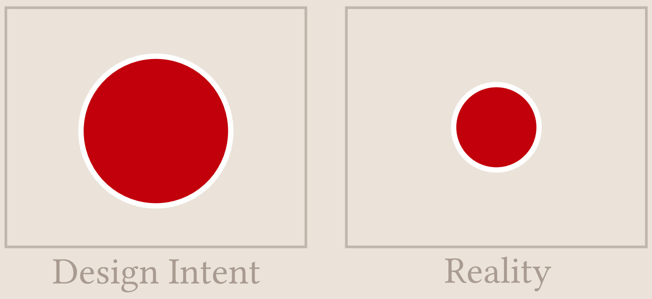
Part Of



Something less than the intent, qualitatively. Think about what system deviations (which cause negative consequences to people) might lead to reductions in achieving the intent.

Only part of the design intent is achieved
by some quantitative decrease

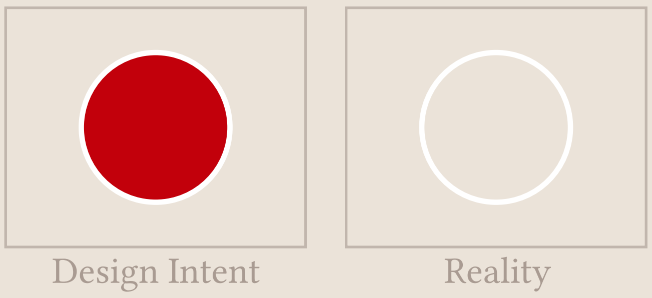
Less



Less of the intent, measured quantitatively (such as count, rate, size, position, duration, other measurable variable). Think about what system deviations (which cause negative consequences to people) might lead to measurable decreases numerically.

No part of the original intent is achieved,
and nothing else is achieved either

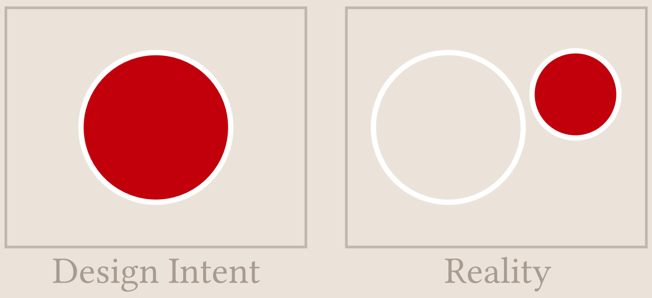
No or Not



The intent is not done/completed. Think about what system deviations (which cause negative consequences to people) might lead to the intent not happening at all or failing completely, and nothing else being achieved either.

No part of the original intent is achieved,
but something else completely different is achieved

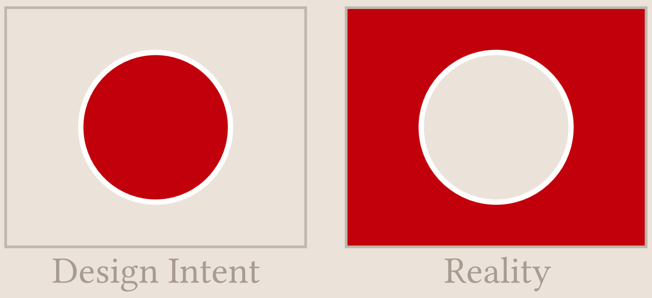
Other Than



Complete intent substitution. Think what deviations (which cause negative consequences to people) might occur/happen in this system leading to something else being achieved instead (not as well as).

No part of the original intent is achieved,
the logical opposite of the intent is achieved instead

Reverse



Logical opposite of the intent. Think what the intent is, then its opposite and what deviations (which cause negative consequences to people) in the system might lead to this.