WHITE PAPER

INTRODUCTION TO CHAZOP: ASSESSING THE RISKS OF CONTROL SYSTEM FAILURE

Peter Clarke PhD

Managing Director, xSeriCon

February 2016

Contact the author: peter.clarke@xsericon.com

Rev: 0.1

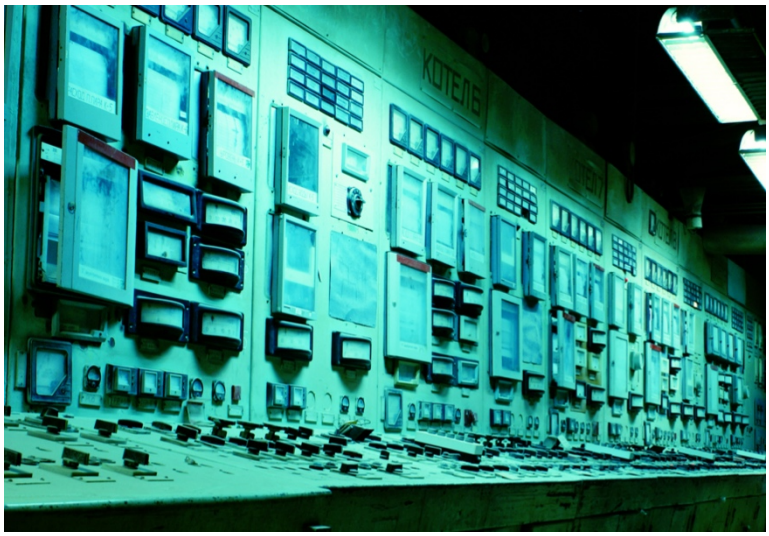
ABSTRACT

Detailed hazard and risk analysis is now routinely performed to assess malfunctions and upsets of process equipment. However, less attention is paid to the potential for upsets in process control systems. This is a risk management vulnerability, as such upsets can lead to major accidents, downtime and lost revenue. Analytical methodologies such as CHAZOP comprehensively address all potential causes of failure, including hardware, software, human factors, cyber security and external factors such as power failure. They highlight areas where unwarranted assumptions have been made, training and management are weak, and single points of failure exist that can lead to a process shutdown.

Based on the author's substantial experience in this area, this paper discusses the justification for performing control system risk analysis; explains how to prepare and develop an efficient CHAZOP study; describes practical tips and pitfalls for executing the study; and explains how to optimise the study's effectiveness.

INTRODUCTION: THE NEED FOR CONTROL SYSTEM RISK ANALYSIS

During the design phase of a new or upgraded process plant, process risk assessment is routinely performed, using widely accepted techniques such as HAZOP [refs 2, 5]. But control system failures are rarely considered at this stage, except in terms of an individual control loop upset during HAZOP. This leaves the plant vulnerable to unmeasured risks. The control system is likely to contain a number of "single points of failure" that can lead to multiple consequences, some of which may be severe. These can impose additional demand on safety systems such as SIS, and this source of demand may not have been taken into account when designing the safety systems. Control system faults may also cause the operator to receive incorrect information, affecting decision making, or even remove the operator's control over the plant entirely.



Unlike HAZOP, control system risk analysis is not yet seen as a normal part of a project's safety lifecycle. This can leave the plant vulnerable to a significant source of risk. A control system risk analysis is appropriate for any project involving a new control system, a significant hardware or software upgrade, or new connections between systems.

This paper provides only a brief introduction to Control Systems HAZOP (CHAZOP), an increasingly popular method of identifying risks associated with control system failure. A more detailed paper [ref 1] is also available from xSeriCon, setting out a range of alternative study methods and a wealth of information on how CHAZOP can be executed effectively.

As well as the process sector, CHAZOP is valuable for many projects in other sectors such as manufacturing, machinery, power, transport, and mining.

WHAT TYPES OF CONTROL SYSTEM RISK ANALYSIS ARE AVAILABLE?

The term CHAZOP (Control systems HAZOP, or Computer HAZOP) has been applied to several types of study, which differ in their objectives and methodology. This section describes the type that is most accurately known as CHAZOP. The other major types are described in [ref 1].

The purpose of CHAZOP is to find possible causes of process upset due to control system failure. CHAZOP can effectively be performed using a 'What-If' procedure. Details are provided in a later section of this paper.

The output of this study is a detailed list of all possible consequences of control system failure, optionally including assessment of the frequencies and severities of the outcomes. This can give a direct indication of whether tolerable risk targets are met; if they are not met, further action will be needed. CHAZOP also provides a wealth of other information including:

- A list of potentially critical failure cases needing more detailed study using LOPA;
- A set of recommendations for design changes or further study;
- A means of determining critical points of failure;
- A list of key safeguards (protective measures) on which the safety of the process is highly dependent;
- The frequency of demand on safeguards that provide a layer of protection against the consequences of control system failures.

One of the key inputs to CHAZOP is a HAZOP report for the process equipment under consideration. CHAZOP should therefore come after HAZOP in the project timeline. Also, CHAZOP yields information needed for the SIL determination study, so CHAZOP should be performed before SIL determination.

If the process includes batch or sequence operations, in addition to the steady-state CHAZOP, it may be appropriate to conduct a step-by-step study for each step of the batch or sequence. This study need only consider the parts of the system whose failure consequence could vary depending on which step is in progress.

The step-by-step analysis can follow the full CHAZOP method, with a cut-down checklist to reflect only the relevant failure modes. Alternatively, if the study team already has substantial experience of operating the sequence, it may be possible to use a brainstorming approach based on 'What If' methodology.

CHAZOP METHODOLOGY: INTRODUCTION

CHAZOP can be seen as a variant of HAZOP. A classic HAZOP study [refs 2, 5] is a workshop activity in which the team first defines the scope of study, and divides it into physical sections called *nodes*. An iterative process is then executed, in which the team:

- selects a node to study;
- selects a 'deviation' (such as No Flow) from a predefined list;
- searches for all possible causes of the deviation (such as a valve getting closed, or a pump stopping) within the node;
- identifies all credible consequences of each cause, assuming there is no system or operator response to the incident and all engineering safeguards (such as trips and relief valves) fail;
- identifies the safeguards provided to reduce the likelihood of the consequences;
- decides whether the risk of harm arising from each cause is tolerable;
- makes recommendations for further study or design changes where required.

The steps above are repeated for all nodes, deviations, causes and consequences identified. All findings are documented as the study proceeds. The entire study can take several days or even weeks to complete.

The author's recommended approach to CHAZOP is similar, except for the first three steps. Instead of nodes, the scope is divided into functional areas (examples are provided in the following section). Instead of deviations, the study uses a checklist of failure classes, such as hardware failure, software error, and power failure. Instead of causes, the team brainstorms a list of potential deviations from normal behaviour, within the scope of each failure class. Each of these is examined in turn. One effective approach is to phrase them as 'What If' questions, such as: 'What if the AC power feed to the main control cabinet is lost?'

It is also possible to conduct CHAZOP using HAZOP-style guidewords; a list of suggested guidewords is provided in [ref 3, page 150].

CHAZOP requires an interdisciplinary team. Most of the information needed relates to electrical, control and data systems, including both system hardware and software and networks. Process engineers and operators may be required from time to time, but not necessarily on a full-time basis. Third party information may be needed if there are critical data connections to outside. Package vendor guidance may be required when studying package PLCs.

In the following sections, we explore each step of the CHAZOP study in more detail.

CHAZOP FUNCTIONAL AREAS

A plant's control system typically consists of a number of distinct systems that are mostly separate in function and architecture. These systems share data through a network. The CHAZOP study can consider each of these systems or functional aspects in turn. Normally the study starts with systems that have the most direct control over hazardous operations, such as the process control system (DCS or BPCS), power systems, networks, tank farm monitoring systems, and truck or ship loading systems. After these are completed, the study considers systems whose failure is less likely to lead directly to a major incident, such as HMIs, remote PLCs, fire and gas monitoring systems and the data historian.

The functional areas can be indicated in various colours on a single-page network diagram, showing each device (PLC, HMI, network switch etc) as a block, interconnected by data-carrying lines. This is equivalent

to marking HAZOP nodes on a Process Flow Diagram (PFD). The marked-up network diagram should be included in the CHAZOP report. Take care to ensure all parts of the system within the scope of the study are considered and marked on the diagram.

Overall, the scope should begin at the main low voltage (110VAC, 220VAC or 415VAC) power feed into the power distribution board for the control system. The scope ends at the I/O connectors that interface to process monitoring and control equipment in the field, such as sensors, limit switches, solenoids, valves and motor control circuits.

INPUT DATA REQUIRED FOR CHAZOP

HAZOP report. The CHAZOP needs to refer to a previous HAZOP study covering the same process area. Before starting the CHAZOP study, the chairman should work through the HAZOP worksheet, identifying all causes relating to control system failures, and noting the maximum consequences. This preparation is important because it allows the team to give definitive answers to the following questions, supported by specific references to the HAZOP worksheet:

- What is the worst-case consequence in the event of any specific type of control system failure?
- If a specific control system failure occurs, does it invalidate any HAZOP safeguards for the scenarios caused by the failure? (This question is, in effect, testing the assumption of independence between cause and safeguard that was made during HAZOP.)
- Are there any pairs of I/O signals that should be assigned to different I/O cards, in order to reduce the impact of a single point failure of one I/O card?
- Could multiple HAZOP scenarios be caused simultaneously by a single control system failure? If so, is there a synergistic effect leading to a more serious overall consequence, such as overloading of the flare system?

Other information required. The following documents should be available during the CHAZOP workshop, preferably as searchable softcopy:

- An approved CHAZOP procedure (similar to a HAZOP procedure)
- Control network diagram (discussed in the preceding section)
- Closeout report for any relevant HAZOP recommendations
- Data sheets for all field equipment connected to the control system, showing full specifications including failure modes (i.e. how the equipment is designed to behave in event of power failure, loss of instrument air supply, etc).
- Data sheets, operating manuals, service manuals, wiring diagrams etc for all hardware within the scope of the CHAZOP study
- Information about power feed architecture (one line diagram or similar)
- Information (or assumed data) about the quality and reliability of services used by the control system, such as power feeds
- Information about any critical data connections to other systems outside the scope of the study, for both inward and outward data flow

Detailed information about software within the control system is usually not required.

CHAZOP FAILURE CLASSES

Instead of applying 'deviations' as in conventional HAZOP methodology, in CHAZOP we can apply a series of 'failure classes', each dealing with one conceptual aspect in which failures may occur.

The following list sets out a tried and tested set of failure classes, [ref 4] along with examples of typical failure scenarios for each (the list of examples is by no means complete). The CHAZOP team should consider each failure class in turn, asking what relevant failure modes exist within the functional area being studied.

As with HAZOP, it is important to identify single, root cause failures. For example, rather than writing "PLC failure" as a cause, break down the scenario to failure of the individual modules such as CPU, memory module, power supply, I/O card, interconnecting cables and backplane.

Power supply. Power loss, power dip, power supply fault, UPS fault.

Hardware failure. Modules, cards, cables, connectors, switches, monitors, keyboards, network equipment.

Communications. Consider network communication failure, and compatibility problems with existing or legacy equipment.

Software. Treat the software as a black box that converts input data to output values. Consider the effect of any false output values the software could produce in the worst case: frozen, high, low, fluctuating or random, bad (meaningless) or no value.

Human factors. Entering wrong values, pressing wrong buttons, failing to take timely actions, overloading, ergonomics, and misunderstanding of information provided by the HMI.

Maintainability and overrides. Can system maintenance be done without disturbing the process? How is software updating controlled? If maintenance overrides are provided, consider what happens if the override is accidentally left in place after the maintenance is completed.

Security. Cyber security, taking into account the possibility of attack (or accidental introduction of harmful software) from inside or outside the organisation. Physical security of network hardware.

Utility failure (other than power). Consider failure or upset of any other utilities such as fire mitigation systems.

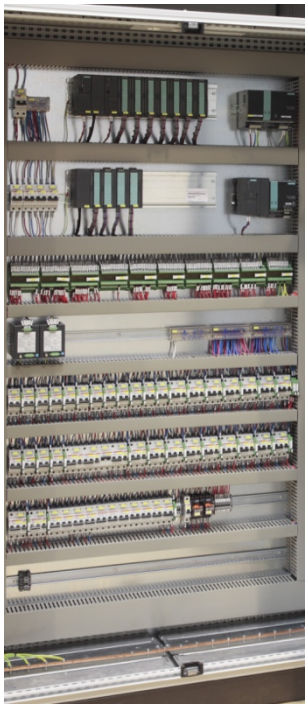
Diagnostics. False alarms from diagnostics built into control systems.

Environmental conditions. Temperature, dust, sandstorm, flood or other reasonably foreseeable environmental condition. HVAC and ventilation fan failure.

Loss of stored data. Hard disk crash or failure of an external resource.

Non-normal operating modes. Consider any specific hazards that exist during non-normal operation, such as startup, shutdown, or emergency situations.

CONSEQUENCES, SAFEGUARDS AND RECOMMENDATIONS



Once the potential failure causes have been identified, the 'reasonable worst case' consequences of each failure are assessed, as in normal HAZOP procedure. Bear in mind that a single cause could lead to multiple consequences. The HAZOP report extract mentioned earlier in this paper will help the team to determine a reasonable consequence for each type of upset.

Safeguards that are able to reduce the probability of the consequence should be identified and documented. In CHAZOP, some safeguards can generally be found in the control system itself (such as redundant components, backup power supplies, and alarms with operator response). In addition, any consequence that impacts the safe operation of the process is likely to have safeguards in the process equipment, such as process alarms, control loops, trips, and relief devices. However, it is important to verify that all these safeguards will remain valid in the failure case under consideration: CHAZOP sometimes reveals situations where a single point failure affects safeguards that were assumed to be valid in the HAZOP study. This can leave the process dangerously under-protected.

Recommendations should be raised if the team identifies cases where the risk may be unacceptable, or where further information or study is needed to confirm the level of risk arising from a particular failure event.

CONCLUSION

A typical CHAZOP workshop takes around 3 days to complete, plus preparation and reporting time. Under the guidance of an experienced and impartial chairman, the study can generate a wealth of valuable information about the weaknesses and vulnerabilities of the control system, highlighting areas where better information is required, and enabling the design and operations teams to optimise the availability of the system. CHAZOP also throws a spotlight on assumptions made about the operation of the system—for example, assuming that an external utility or source of data is 'always' available—and allows the team to examine whether these assumptions are justified. For a relatively small investment of manpower, CHAZOP can yield great benefits in terms of plant safety and system performance.

REFERENCES

1. Clarke, P., CHAZOP: Assessing the risks of control system failure, 2016, xSeriCon, available from www.xsericon.com
2. Crawley, F., Preston, M. and Tyler, B., HAZOP: guide to best practice, 2nd edition, 2008, Institution of Chemical Engineers.
3. Cameron, I. and Raman, R., Process systems risk management, 2005, Elsevier.
4. Andow, P., Guidance of HAZOP procedures for computer-controlled plants, Health & Safety Executive contract research report no. 26/1991.
5. Kletz, T., Hazop and Hazan: identifying and assessing process industry hazards, 4th edition, 1999, Institution of Chemical Engineers.

GLOSSARY OF TERMS USED

BPCS	basic process control system
CHAZOP	control systems HAZOP (or computer HAZOP)
CPU	central processing unit
DCS	distributed control system
HAZOP	hazard and operability (study)
HMI	human-machine interface
HVAC	heating, ventilation and air conditioning
I/O	input/output (card or module)
LOPA	layer of protection analysis
PFD	process flow diagram
PLC	programmable logic controller
SIL	safety integrity level (a reliability measure)
SIS	safety instrumented system, also known as ESD system
UPS	uninterruptible power supply

For further guidance and training on all the topics covered in this paper, including CHAZOP, HAZOP and other risk analysis techniques, or to enquire about consultancy services, please contact xSeriCon: +852 2633 7727 | peter.clarke@xsericon.com | www.xsericon.com