THE ARROW

STPA: A Systems Approach to Process Hazard Analysis

The Problems with Traditional Methods of Process Hazard Analysis

Traditional methods of process hazard analysis (PHA), such as HAZOPs, FMEAs, and others, use a divide and conquer approach. They break down the system into nodes or components and analyze each part separately, to provide an assessment for the entire system. This approach assumes that when a system is broken down into its component parts, its properties are not significantly changed. But as our projects have become increasingly complex, this assumption has become increasingly questionable. Systems effects may well be missed.

Further, traditional PHA methods assume that accidents are caused by component failures. But accidents can happen even if no component fails, especially in complex systems. Safety is an emergent property. It cannot be fully understood at the component level, but arises out of complex interactions of multi-component systems.

What is STPA & How Does it Help Us?

Systems Theoretic Process Analysis (STPA) is a systems approach to hazard analysis. It is based on the premise that accidents happen when we lose control. They are a control problem, not a failure problem.

STPA is a structured approach that systematically decodes hazards related not only to component failures, but also to component interaction failures, flawed controller requirements, human error, design errors, and more.

Before an STPA is Performed

In our two previous Arrow articles, we covered the Stream-based HAZOP method and using the GATE risk ranking methodology that replaces the color-coded matrix with a Required Risk Reduction (RRR) matrix.

STPA is the third phase in the GATE Risk Management process. Significant risks identified in the HAZOP are studied further using the STPA methodology. It applies the most rigorous hazard assessment methodology currently available to the most significant hazards.

Steps to Performing an STPA

Step 1: Defining System Boundaries, Losses of Concern, & Hazards

System Boundaries: An important thing to remember is that an STPA should not be performed on a 'part of the system'. Breaking down a system into small nodes will render the STPA performed useless! We need to consider the 'entire' system.

Losses: The first step is where we define the losses of a system. A loss can be anything that is unacceptable to stakeholders, such as:

- Loss of Life or Injury
- Downtime
- Loss of Intellectual Property
- Environmental Damage, etc.

Hazards: Next, we determine hazards that lead to the losses identified.

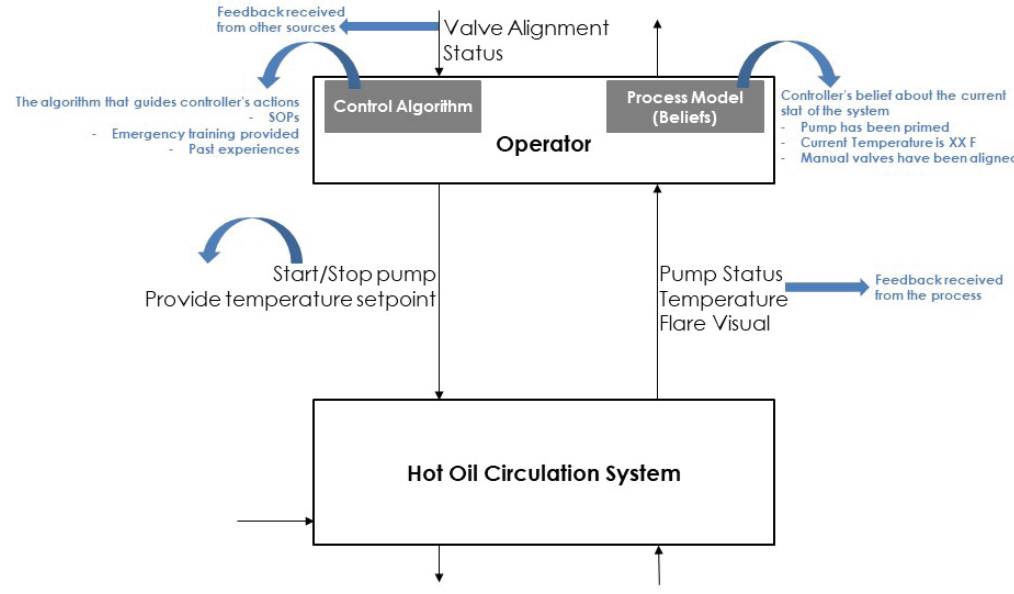


Figure 1: Example Control Loop (with a Human Operator as a Controller)

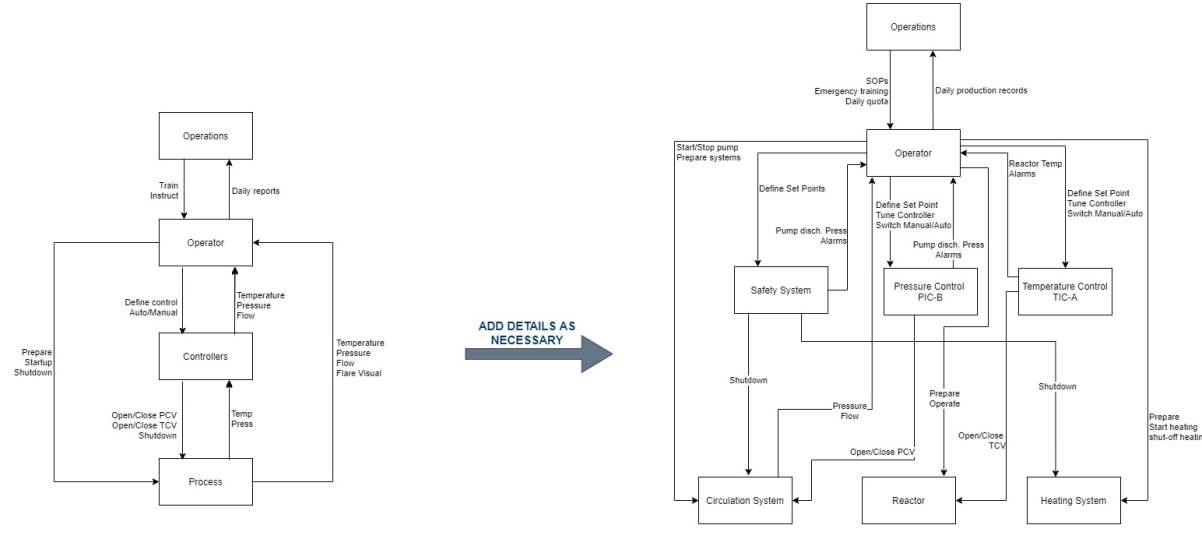


Figure 2: Control Structure in Development

Step 2: Modeling the Control Structure

Every process is controlled via certain 'control actions', like opening a valve, starting a pump, providing a controller set point, and so on.

STPA analyzes such direct control actions to realize scenarios in which a particular action, or failure to act, can become unsafe. Such an analysis is performed using control structures.

Each Controller consists of a Process Model and a Control Algorithm.

The Process Model uses the feedback provided by the process, or elsewhere, to determine the controllers 'beliefs' about the state of the system.

The Control Algorithm determines the controller's response to its 'beliefs'. For a human controller, the control algorithm could be SOPs or simply their understanding of the process. For an automated controller it is usually a PID controller algorithm.

Errors can come from flawed feedback, flawed process model, flawed controller algorithm/ response, etc.

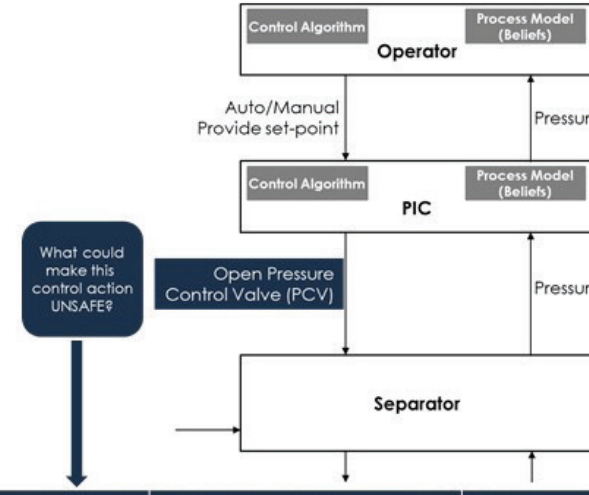
A control structure is a combination of all the control loops that exist in a system, arranged hierarchically. The control structure elucidates the hierarchy of control (who overrides whom?) and also clearly defines the influences different components have on each other. STPA uses such control structures to study processes. This makes it possible to identify hazardous system interactions and realize any missing controller requirements. Figure 2 shows a control structure for a hypothetical process at 2 levels of detail.

A fully developed control structure will include every control action that is enforced on the process, all possible feedback received from the process, and every responsible party.

Step 3: Identifying Unsafe Control Actions (UCAs)

Once the control structure is developed, every control action is studied to realize possible ways in which it could lead to a hazard, as seen in Figure 3. To do this, we ask four questions:

1. How does providing this control action cause a hazard?
2. How does not providing this control action cause a hazard?
3. How does providing this control action too early/too late cause a hazard?
4. How does providing this control action for too long or stopping it too soon cause a hazard?



Not providing CA causes hazard	Providing CA causes hazard	CA provided too early/too late	CA stopped too soon/ applied too long
UCA-1) PIC does not provide Open PCV command when pressure in the vessel exceeds set-point, causing over-pressure and production shutdown. (Hazards 1,3)	UCA-2) PIC provides Open PCV command when the downstream compressor has not been loaded and is not ready to start. (Hazards 1,2,3)	-	UCA-3) PIC stops providing Open PCV command before pressure in the vessel reaches set-point, causing over-pressure and production shutdown. (Hazards 2,3)

Figure 3: Identifying Unsafe Control Actions

Step 4: Identifying Causal Scenarios

Once all the ways in which control actions become unsafe are recognized, scenarios that could lead to such unsafe control actions are identified. We do this for every unsafe control action, one at a time, by going around the relevant control loop, and brainstorming how different parts of the loop can be responsible for the unsafe control action. See an example in Figure 4.

Once causal scenarios are identified, recommendations can be made to prevent them, and hence prevent any resulting unsafe control actions. This is how an STPA helps us design safer processes.

Viking Can Help

We are on a mission to improve the way industry does process hazard analysis.

With our legacy of experience in process design, materials selection, risk assessment and systems analysis, we can provide effective and efficient design, fabrication, and operational support as the energy industry moves into a renewable future.

Article By: Pranav Kalantri
with Viking Engineering

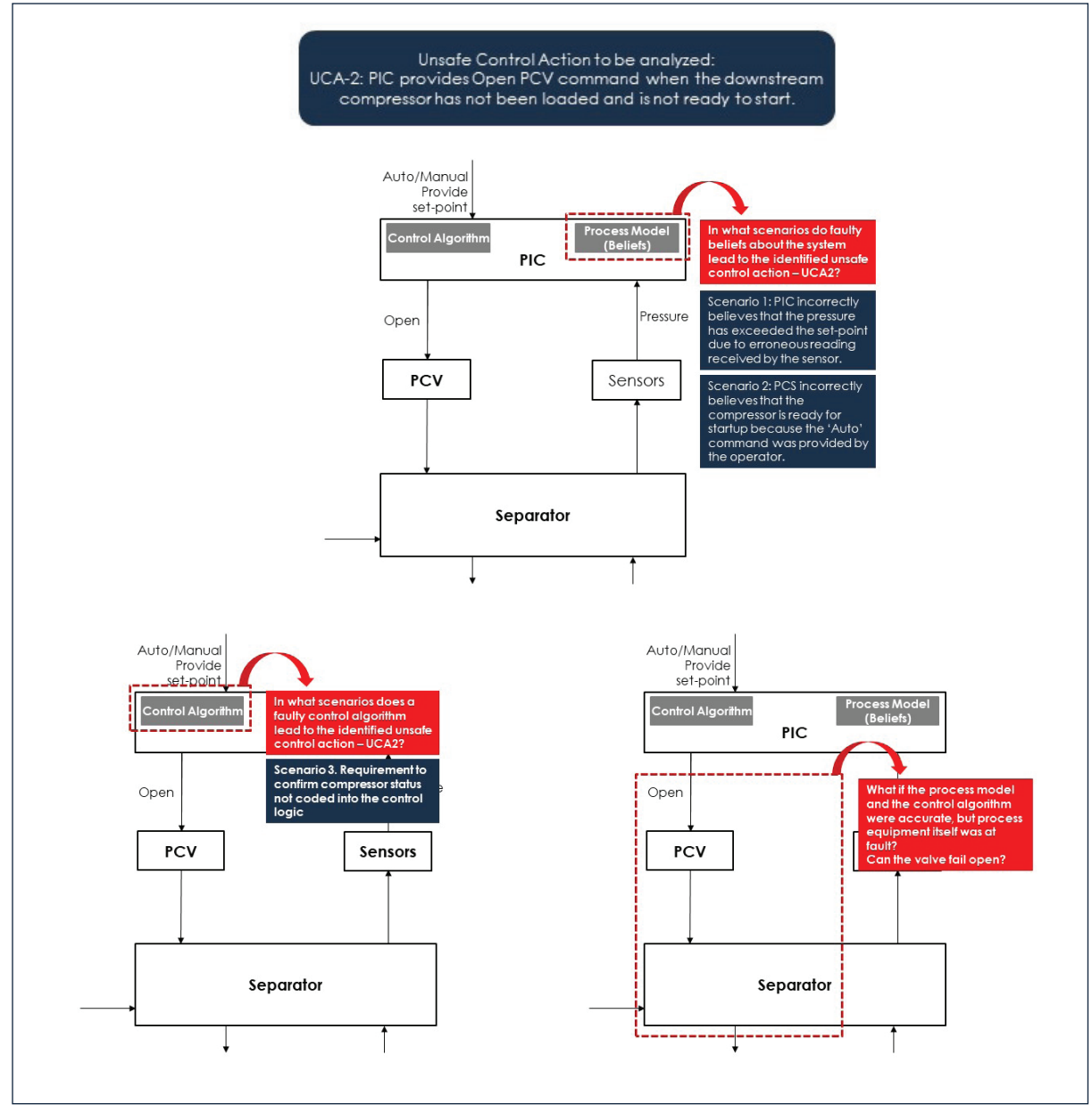


Figure 4: Identifying Loss Scenarios