Using STPA and CAST to Design for Serviceability and Diagnostics

by

Hannah M. Slominski

Bachelor of Science in Mechanical Engineering
Purdue University, 2006

Submitted to the System Design and Management Program
in Partial Fulfilment of the Requirements for the Degree of

Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology
May 2020

Signature of the author_____
System Design and Management Program
May 8, 2020

Certified by_____
Nancy G. Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Supervisor

Accepted by_____
Joan S. Rubin
Senior Lecturer and Executive Director
MIT System Design and Management Program

Page intentionally left blank

Using STPA and CAST to Design for Serviceability and Diagnostics

by

Hannah M. Slominski

Submitted to the System Design and Management Program on
on May 8, 2020 in Partial Fulfilment of the Requirements of the Degree of
Master of Science in Engineering and Management

Abstract

OEM industries are facing increased challenges providing proactive and reactive equipment support. Increased product complexity and the fast rate of technology change make problems difficult to understand, prevent, and resolve. The cost of machine unavailability is extreme, and reliability-based design methods ignore service time as a key contributor to machine unavailability. Serviceability and diagnostics are an important control to minimize customer losses when problems do occur. Methods are needed that identify serviceability needs early in the product development process while managing product complexity.

STAMP (System-Theoretic Accident Model and Processes) is an accident causality model developed as a new engineering approach to system safety. While it was originally created for safety, its foundation in systems theory lends itself to other emergent properties, like serviceability. This research demonstrates that STAMP techniques can be applied to address existing serviceability issues and to guide service-friendly system design in early, conceptual design phases.

Two case studies, drawn from industry, are explored to verify the effectiveness of applying STAMP to serviceability. Both case studies successfully generated hardware, software, and operator interface design requirements. They also produced recommendations for the product development and support processes. By using STAMP techniques to understand system interactions and strengthen service control structures, OEMs can address many of the challenges they are currently facing providing serviceability and support.

Thesis Supervisor: Nancy G. Leveson
Title: Professor of Aeronautics and Astronautics and Engineering Systems

Page intentionally left blank

Acknowledgements

Wow, what a journey! In the last two years, I became a mother, moved across country twice, completed a master's degree from MIT, and worked full time. I could not have done this (and stayed as relatively sane as I did) without the unwavering support of my husband, Cary. Thank you for always believing in me and encouraging me on this journey. You give me the strength and courage to take on new challenges. Thank you to my son, Eli. Although you're only eighteen months old, you already show great resilience and flexibility. You've faced every change with bravery and ease. Thanks to my family for joining me on my Cambridge adventures and giving up your space to live in campus family housing! I love you both and can't wait to see what future adventures we'll have together.

I also want to thank my parents and all my other family that supported me in this endeavor. Mom and dad: From watching Eli while I worked on my thesis to feeding us several nights a week, thank you for all of your support. Thank you to mom, Jody, and Stacey, three strong women in my family who completed the working-professional, master's-student, motherhood-journey before me. You inspired me and showed me what's possible. Matt, thank you for the words of encouragement when I was overwhelmed by my thesis.

Thank you to my advisor, Nancy Leveson. Your writing and teachings taught me a new way to see the world. I see and think in control/feedback loops now - the verdict is still out how much my family appreciates my new way of thinking! New perspectives can be hard to come by as mid-career engineer. You gave me a new lens and re-energized me to tackle big, engineering challenges.

To the SDM director, Joan, thank you for personally welcoming me the first week of boot camp and offering your help and support. I wasn't sure how I was going to manage school with a new baby, but you gave me the confidence to charge ahead. Thank you for guiding my SDM path and always being there for an encouraging drop-in office chat!

Lastly, I want to acknowledge Candi, Anne, Megan, Rachel, and all of the people who provided input on my thesis and case studies. Thank you Candi for helping make MIT possible and looking out for my best interests. Thank you to my wonderful employer who demonstrates commitment to employee development.

Page intentionally left blank

Table of Contents

Table of Figures

Table of Tables

List of Acronyms

AST	Automatic Shift Transmission
PST	Power Shift Transmission
CHS	Contribution to Hazardous State
CAST	Causal Analysis based on System Theory
DA	Diagnostic Address
DR	Diagnostic Receptacle
DTC	Diagnostic Trouble Code
FMEA	Failure Modes and Effects Analysis
MG	Main Gearcase
OEM	Original Equipment Manufacturer
RCM	Reliability Centered Maintenance
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TAC	Technical Assistance Center
TM	Technical Manual
UCA	Unsafe/Unserviceable Control Action

1 Introduction

1.1 Motivation

The agricultural and construction industries are facing increased challenges providing proactive and reactive equipment support. Increased product complexity and the fast rate of technology change make problems more difficult to understand, prevent, and resolve. The remote locations of many farms and construction worksites can lead to significant downtime waiting for technicians and parts. Across the industry, service technicians are increasingly harder to recruit and retain, and many areas are dealing with technician shortages. At the same time, the cost of machine unavailability is increasing due to increasing labor costs, equipment costs, and equipment size. When combined, all these factors result in an urgent need to improve product serviceability and diagnostic capability.

As equipment complexity and the rate of technology change increases, problems are increasingly more difficult to isolate and resolve. As shown in Figure 1, manufacturer data indicates that the time required to troubleshoot and repair machine problems has doubled over the last decade. At the same time, service support calls (TAC cases) have quadrupled, indicating that product complexity has outpaced product serviceability. Methods are needed that identify serviceability needs early in the product development process while managing product complexity.

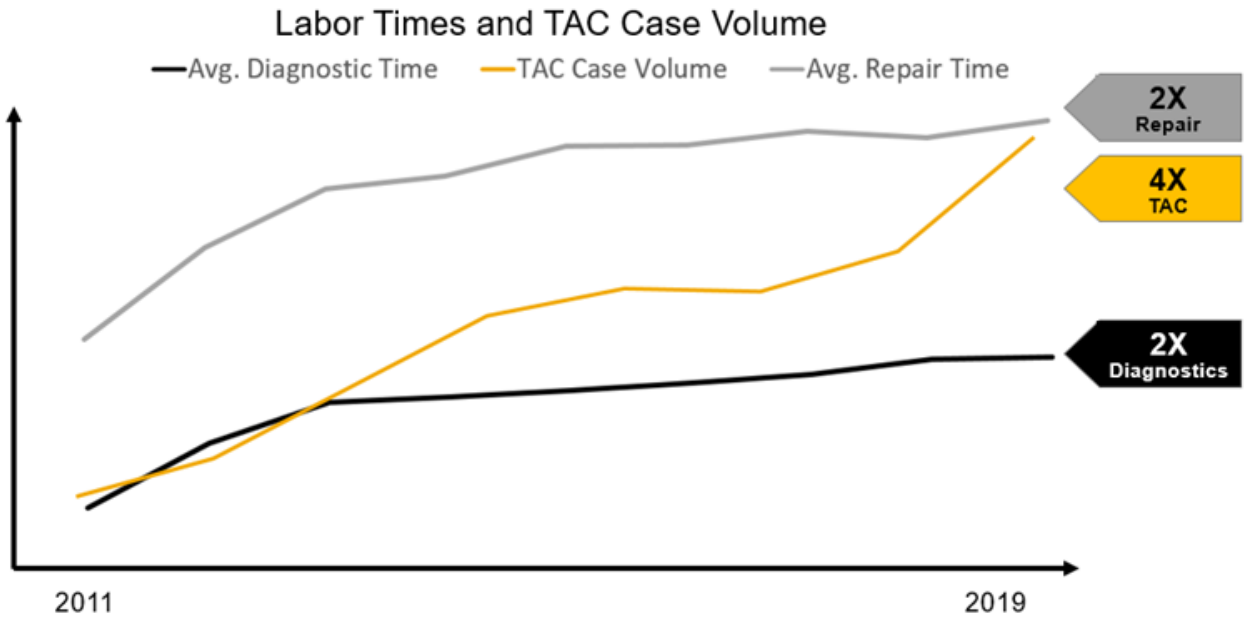

Figure 1: Labor Times and Service Support Call Trends

The objective of repair and diagnostics is to restore a product to an operational state after a problem occurs, also known as corrective serviceability or corrective maintenance. Repair and diagnostic

activities may include troubleshooting, removing and replacing components, repairing and adjusting components, and updating software. While other factors such as reliability, preventative maintenance time, and logistic support time affect machine availability, the focus of this research is on corrective serviceability.

Reliability is critical to uptime and productivity; however, when problems do occur, operators and technicians need to be able to detect the problem and identify appropriate mitigation actions quickly to reduce downtime and minimize repair costs. Time spent repairing and troubleshooting problems results in machine unavailability and financial losses to the farming or construction operation. It shifts scarce technician labor time away from value added services, reducing dealer profitability. It also adds cost to equipment manufacturer through warranty reimbursement. Ineffective product serviceability can drive the unnecessary replacement of functioning parts, create secondary failures or machine damage, and require multiple service technician trips to resolve issues, increasing logistic response time. It's important that serviceability is considered during the design to avoid these customer, dealer, and manufacturer pain points.

Across the industry, there is a shortage of skilled service technicians. Equipment retailers and service shops are dealing with challenges finding qualified applicants for service-related positions. According to a survey of agricultural retailers conducted by South Dakota State University, over 78% of respondents indicated it's either difficult or very difficult to find qualified applicants or that there are no qualified applicants in their area (Erickson, Fausti, Clay, & Clay, 2018). With equipment complexity increasing, many farm and construction operations rely heavily on dealerships and third-party service shops to troubleshoot and repair equipment. The demand for more services combined with the service technician shortage, increases the value of a service technician's time. Quick and easy serviceability reduces technician labor time required, reducing the cost of service. It also frees up valuable service technicians to provide additional services to more customers, improving service shop and dealer profitability.

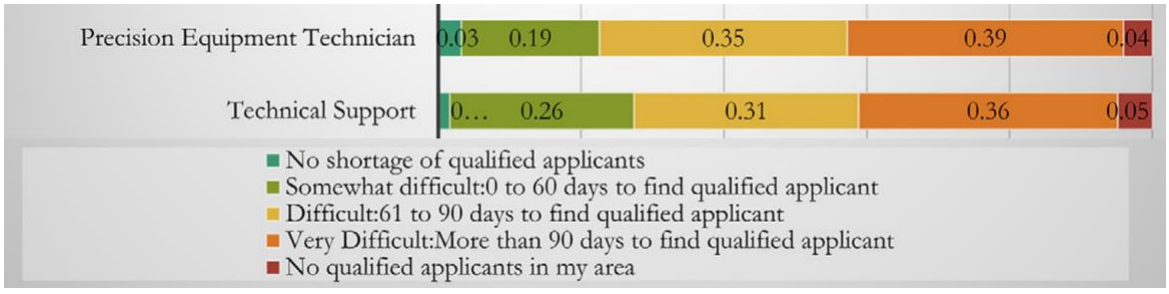

Figure 2: Agriculture Equipment Retailer Survey Results (Erickson et al., 2018)

An easily serviceable product saves initial production costs as well as service and support costs. Designed in self-diagnostics, tests, and condition monitoring reduce manufacturing effort (Blanchard, Verma, & Peterson, 1995). Easy to access components, designed-in lifting points, and use of standard, shared hardware also reduce manufacturing time and the need for costly fixtures and special tools. Avoiding special tools saves factory costs and repair shop costs. If an assembler or service technician doesn't have a required special tool available when needed, they may do the task without the tool. Not only do special tools add cost, they can lead to inadequate repairs, damage to unrelated systems, and follow-on problems.

Increased product complexity affects the service technician and operator's abilities to identify problems and complete the repair required. Over-alarming the operator can lead to alarm fatigue, a condition where the alarms are ignored or not understood by the operator. If a valid alarm is ignored, equipment damage may occur, leading to machine unavailability. When the equipment can't detect or isolate problems through self-test capabilities, troubleshooting is left up to the service technician. This increases service time and may lead to guess-and-check troubleshooting, where parts are swapped until the problem is resolved. Swapping parts before confirming the repair required is often referred to as "swapnostics", and it's increasingly common on large agriculture and construction equipment.

Another key motivation for this research is that highly complex products are increasingly difficult to design. Systems engineering and architecture techniques exist to manage this complexity, but there are a lack of methods focusing on how to design for serviceability, maintainability, and diagnosibility. Engineering teams are challenged to satisfy a slew of emergent property requirements such as safety, manufacturability, compatibility, and reliability. When serviceability requirements are difficult to identify or identified too late, other requirements may take precedence due to development pressures. All of this leads to a need for Design for Serviceability methods that can be used early in the development process while handling product complexity and optimizing engineering effort.

1.2 Thesis Objectives and Approach

The purpose of this research is to improve product serviceability by identifying systems-theory based methods for generating serviceability requirements and recommendations leveraging STAMP techniques. STAMP (System-Theoretic Accident Model and Processes) is an accident causality model developed as a new engineering approach to system safety. Causal Analysis based on STAMP (CAST) and System-Theoretic Process Analysis (STPA) are safety techniques developed to apply the STAMP system safety approach. While these techniques were originally created for safety, their foundation in systems theory lends itself to other emergent properties, like serviceability.

As STPA and CAST are applied more frequently across OEM industries for safety analyses, can similar techniques be used to improve product serviceability? Traditional analysis techniques like Failure Modes and Effects Analysis (FMEA) and fault trees are cumbersome and focus only on component failures. Other methods, such as serviceability reviews, rely on virtual or physical parts. While serviceability reviews are useful for verification, they are too late in the design process to be an effective requirement-identification method. Can STPA efficiently and effectively provide serviceability recommendations into the product design and hierarchical service architecture? Can CAST be used to analyze serviceability issues and generate recommendations not only for the physical design, but for the larger sociotechnical system including the product development process?

As engineering resources are increasingly limited and product development timelines are condensed due to customer demands, aligning stakeholder needs can be an efficient way to reduce coordination efforts and manage product design trade off decisions. Can safety STPA control structures be reused and leveraged for serviceability, reducing engineering effort to design for serviceability? If STPA can be applied to serviceability, what analysis modifications or extensions are required?

A literature review was conducted to understand the history of design for serviceability within systems engineering and to identify existing design for serviceability techniques. The research also explored STAMP as applied to safety and discovered STPA extensions applied to other emergent properties. This research identified gaps in existing systems engineering serviceability methodologies and framed how design for serviceability can be applied as an STPA extension.

Two case studies, drawn from industry, are developed to verify the effectiveness of extending STAMP to serviceability. One case study leverages CAST (Causal Analysis based on System Thinking) to investigate a current serviceability issue. This case study demonstrates how CAST can be used to identify why the existing product and hierarchical system controls did not effectively prevent the serviceability issue. The CAST case study also generates recommendations for potential changes to the product and hierarchical control structure to enable more serviceable future products. The second case study investigates a future system currently being designed. Safety STPA is applied to determine the system safety constraints and recommendations. After completing the safety STPA, the analysis is redone focusing on serviceability. The STPA case study identifies potential safety and serviceability requirements. These case studies demonstrate that STAMP can be extended to serviceability and identify any modifications required to fit it to serviceability.

1.3 Thesis Structure

Introduction: This section summarizes the motivation for the research and highlights the importance of serviceability in the construction and agricultural industries. This section also defines the research purpose and key questions the research seeks to address. The research methodology is outlined, including a description of the case studies explored.

Literature Review: This section summarizes other research applicable to the purpose of this thesis and identifies where other research can be leveraged and built upon to achieve the purpose. Four main topics are explored as part of the literature review: serviceability as an emergent property, design for serviceability methods, system-theoretic accident model and processes, and STPA extensions to non-safety emergent properties.

Case Study 1: Applying Diagnostic CAST to Existing Issue: This section analyzes an existing diagnostic issue using CAST methodology. The purpose of the section is to demonstrate that CAST is an effective technique for identifying serviceability improvements to the physical design and to the hierarchical service control structure.

Case Study 2: Serviceability STPA of Future System: This section applies STPA to design serviceability into a future system. The case study generates software and hardware design requirements as well as recommendations for the system development process. Through the requirements generation, the case study demonstrates that STPA is an effective "design for" serviceability method.

Recommendations and Conclusions: This section summarizes the research purpose and findings. It addresses the research questions posed and includes insights gained during the case studies. This section includes recommendations that can be used when applying STAMP techniques to future serviceability analyses.

Appendices: The appendices include additional case study details excluded from the main sections.

2 Literature Review

2.1 Serviceability as an Emergent Property

Emergence is a fundamental systems theory concept important to understanding how serviceability provides value. In systems theory, systems are considered as a whole made of interacting parts. When system components interact, behaviors "emerge" that cannot be understood exclusively by considering the behaviors of the individual components (Walden, Roedler, Forsberg, Hamelin, & Shortell, 2015). This theory of emergence can be traced back to Aristotle and is conveyed in a common phrase: "the whole is more than the sum of the parts."

Attributes that emerge over time as a system operates are referred to as emergent properties, or "ilities." Common emergent properties include reliability, safety, manufacturability, and serviceability. Emergent properties capture stakeholder needs beyond the primary functional purpose of a system, and it's critical they are considered during system design and architecture. Emergent properties are collective behaviors of the system, so when a system is decomposed emergent properties are missed. Designing for emergence requires aggregation and considering the whole system context. In agriculture and construction, serviceability is an emergent property that must be integrated into system requirements to ensure customer satisfaction, minimize unplanned downtime, and reduce lifecycle costs.

The definition of serviceability, also known as maintainability, varies across industries and literature. Some literature limits maintainability to corrective actions needed to get a system back up and running after a problem occurs, also known as diagnostics and repair. Corrective maintenance includes isolating the source and correcting the problem (Pecht, 2009). Other maintainability definitions widen the scope, including predictive, preventative, and corrective actions. Preventative maintenance includes scheduled maintenance, condition monitoring used to predict problems before they cause downtime, and the associated proactive service tasks to resolve impending problems (Blanchard et al., 1995). For the purpose of this thesis serviceability consists of:

- Predictive maintenance: condition monitoring that predicts problems before they occur and identifies preventative maintenance required.
- Preventative maintenance: scheduled service tasks that prevent problems and prolong the life of the product (for example, changing engine oil or checking tire pressure)
- Corrective maintenance: unscheduled tasks that restore a product to an operational state after a problem occurred, includes diagnostics and repair.

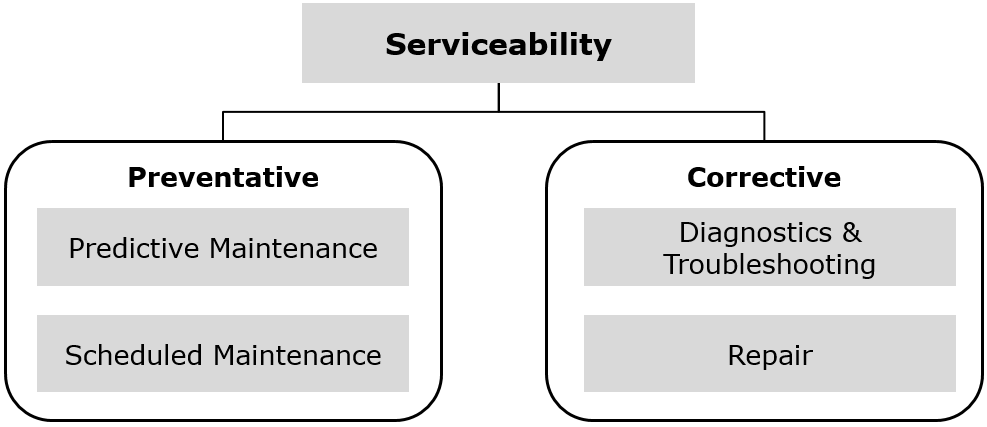

Figure 3: Elements of Serviceability

Serviceability can be expressed as the ease and economy of service tasks. It is often measured in terms of labor hour time, scheduled maintenance frequency factors, and service cost (Blanchard et al., 1995). While improving the ease and economy of preventative maintenance is important to reducing lifecycle costs, preventative maintenance can be scheduled and does not affect unplanned machine unavailability. To minimize downtime and labor costs, the primary goal of diagnosibility is to reduce troubleshooting time. This entails detecting all problems as soon as they occur, isolating the cause, enabling the operator to take appropriate action (for example, turning off the equipment to prevent further damage), and correctly identifying the repair required. Problems can be detected by the machine or by the human operator. Either way, system design criteria should define automatic or manual troubleshooting procedures that confirm the problem prior to repair and minimize diagnostic time.

Over the last 50 years, interest and research in serviceability has increased. Research by de Weck et al analyzes the prevalence of various emergent properties over time and identifies relationships between different emergent properties. As shown below in Figure 4, safety, quality, and reliability have a long history in engineering, while other emergent properties such as maintainability, modularity, and scalability didn't receive much attention until mid-century (de Weck, Ross, & Rhodes, 2012). The first maintainability papers from the 1950's are mainly related to electronics and military equipment. However, as systems become more complex, operational downtime is more expensive and difficult to mitigate. Because serviceability directly affects operational downtime, it is understandable that focus on it has increased in the last 50 years.

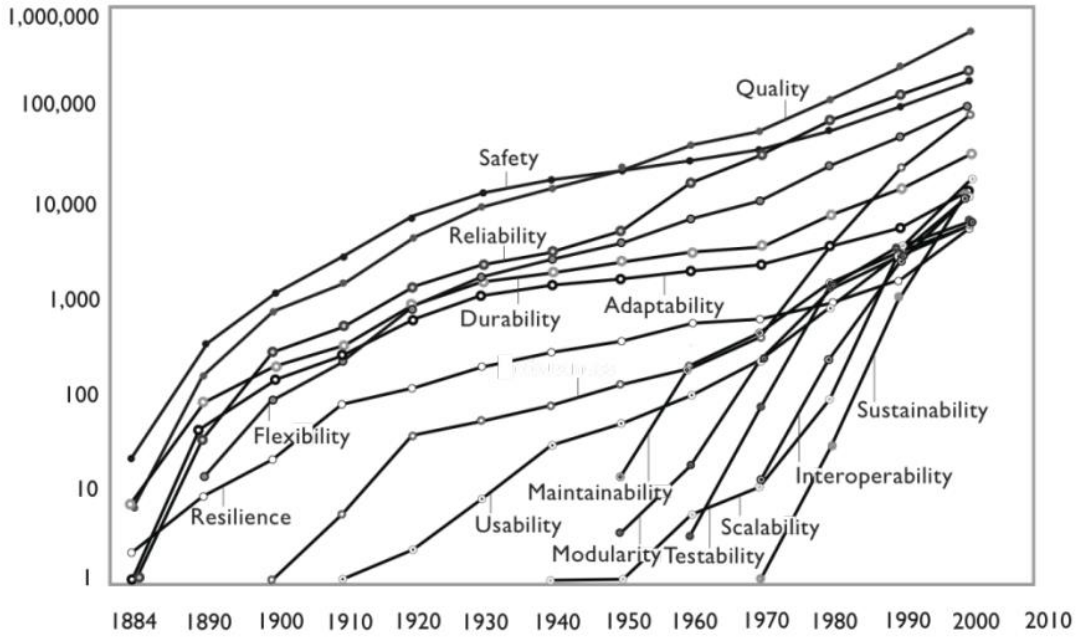

Figure 4: Frequency of Ilities Mentioned in Literature (de Weck et al., 2012)

2.2 Design for Serviceability Methods

The research indicates that while serviceability is accepted as an important emergent property, deserving of systems engineering focus, few methods exist to identify the system and subsystem level serviceability design requirements. Two main categories of design for serviceability methods were found:

- Service and Diagnostic Failure Modes and Effects Analysis
- Reliability Centered Maintenance (RCM).

Both of these methods are based on Failure Modes and Effects Analysis (FMEA). The following subsections present these methods and explore their limitations.

2.2.1 FMEA

FMEA was developed in the 1950's at Grumman Aircraft Corporation (Bowles, 2003). From the 1970s through the 1990s, it was widely adopted across manufacturing industries and standardized, such as in the military standard MIL-STD-1629 (*MIL-STD-1629:*1980). Over the years, various forms of FMEA and FMEA extensions were developed to accommodate different use cases. For example, design FMEAs focus on a product including the parts and components, process FMEAs focus on the manufacturing process, application FMEAs focus on the downstream customer processes, and service FMEAs focus on field service after sales (Dyadem Press, 2003).

FMEA is a bottom up procedure organized around failure modes. The FMEA process analyzes each component using a single-point failure approach and links the failure modes to causes and effects of the failure (Rhee & Ishii, 2003). FMEA considers how the component can fail and determines how that failure can affect the function of the system (Bowles, 2003). Then it estimates the risk in terms of Risk Priority Number (RPN) that is a product of the following ratings: the severity of the failure, the probability of the failure causes, and the likelihood of detecting the failure with the current design controls (Dyadem Press, 2003). The design team uses the calculated risk to prioritize recommended actions. The goal of the FMEA is to identify failure modes and recommend ways to design out the failure mode or mitigate the effects of a failure.

The following steps are performed in an FMEA study (Dyadem Press, 2003), and a typical FMEA worksheet is shown in Figure 5.

- Define the item being analyzed
- Define the functions being analyzed
- Identify all potential failure modes
- Determine causes of each potential failure mode
- Identify effects of each failure mode
- Identify and list the design controls for each failure mode
- Determine recommended actions based on the risk

												Action Results			
Item/ Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause of Failure(s)	Prob	Current Design Controls	Det	RPN	Recommended Actions	Responsibility & Target Completion Date	Actions Taken	New Sev	New Occ	New Det	New RPN

Figure 5: Typical FMEA Worksheet (Pecht, 2009)

While many companies use FMEA to understand and mitigate potential product failures, most are not completely satisfied with the methodology (Pecht, 2009). When FMEA was developed and gained popularity, systems were significantly less complex and were primarily electromechanical. It's no wonder that in today's software intensive systems, with thousands of components and complex interfaces, FMEA is inadequate. FMEA focuses on component failures and FMEA assumes that all failure effects are addressed and fully mitigated through the design (Barkai, 1999). In reality, the users deal not only with failures, but with software flaws, environmental variations, functional degradation over time, and human interactions. FMEAs don't manage abstraction well, and analysis of complex systems with a large number of entities, interfaces, and functions can be tedious and difficult (Dyadem Press, 2003). Failures can only be analyzed one at a time, so compound failure effects are not recognized and their

interdependence is ignored. As previously discussed, behaviors emerge when a system is brought together through the interactions. FMEA is insufficient in dealing with emerging behaviors. Lastly, FMEA relies on a previous understanding of failure modes, and it does not identify unknown failure modes. In today's complex systems that exceed the understanding of a single person, emerging undesirable behavior must be considered – whether it stems from a known or unknown causal factor.

2.2.2 Service and Diagnostic FMEA Extensions

Extensions of FMEA exist that focus on incorporating serviceability and diagnostics into the FMEA process. Traditional FMEA seeks to design out failures and mitigate the effects of failures. Service and diagnostic FMEAs focus on minimizing the impact to machine availability when failures do occur. Service and diagnostic FMEAs typically require conducting an FMEA, then developing serviceability design requirements that prevent or correct the potential problems identified in the FMEA (Blanchard et al., 1995).

A few selected examples of serviceability-related FMEA extensions include the following:

- Using a cost based FMEA to enhance reliability and serviceability (Rhee & Ishii, 2003)
- Automatic Generation of a Diagnostic Expert System from Failure Mode and Effects Analysis Information (Barkai, 1999)
- Using a failure modes, effects, and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems (Goble & Brombacher, 1999)

Rhee and Ishii's research leverages Life Cost-Based FMEA that measures risk in terms of cost (Rhee & Ishii, 2003). This approach seeks to address limitations with how traditional FMEA measures risk, using subjective RPN. It also broadens the scope of the process to consider the overall lifecycle cost and includes several service-related lifecycle cost contributors:

- Detection Time: Time to detect the failure and diagnose the cause
- Fixing Time: Time to fix or repair the problem
- Delay Time: Time for non-value activity such as waiting for people or parts

Life-Cost based FMEA incorporates service labor and part costs. This increases awareness of serviceability needs and captures the effect of service on machine availability and lifecycle costs. However, it does not address fundamental limitations of FMEA such as reliance on subjective probability estimates, focus on known failure modes, and inability to handle complex, software-intensive systems.

In 1999 Barkai demonstrated a way to incorporate repair and maintenance information into an FMEA worksheet, then derive a diagnostics decision maker from the diagnostic FMEA. Information

such as field replaceable component objects, symptoms of malfunctions, repair objects such as part replacements and adjustments, and test objects that obtain information and reason about the state of component objects were documented and incorporated into a diagnostic FMEA worksheet (Barkai, 1999). Figure 6 illustrates a base FMEA worksheet used as an input to the analysis. Barkai then converted the FMEA information into a diagnostic FMEA worksheet as shown in Figure 7.

Item / Functions	Potential Failure Mode	Potential Failure Effect(s)	Sev	Potential Cause(s)/ Failure Mechanism(s)	Occur	Detec	RPN
P2-A02 / +5V output power to Rotary Sensor	Open Circuit	Won't shift out of neutral. If in Forward, when fault is detected, reverts to neutral.	8	Broken wire Connector not properly assembled Contamination/moisture in connector No signal from controller A02 Open circuit in sensor	2	3	48
	Intermittent Open Circuit	Accelerates/decelerates at frequency of intermittence.	8	Broken wire Connector not properly assembled Contamination/moisture in connector	2	3	48

Figure 6: FMEA Worksheet (Barkai, 1999)

Symptom	Detection		Cause				P
	Originating Unit	Activation	Component	Ref. Des.	Failure Mode	Cause	
Won't shift out of neutral	A02	Voltage < +1.5V	Harness	WHA02	Open Circuit	Broken wire	4
					Short to Ground	Pinched Wires	5
					Short to B+	Pinched Wires	5
			Connector	P2	Open	Bad assembly	5
						Contaminated	
			Controller	A02	Short (Int.)		2
					Open (Int.)		
			Sensor	S11	Short (Int.)		2
					Open (Int.)		

Figure 7: Diagnostic FMEA Worksheet (Barkai, 1999)

The diagnostic FMEA information was then input into an off-the-shelf model based diagnostic expert system, that created a diagnostic logic tree, shown in Figure 8, to be used for troubleshooting failures.

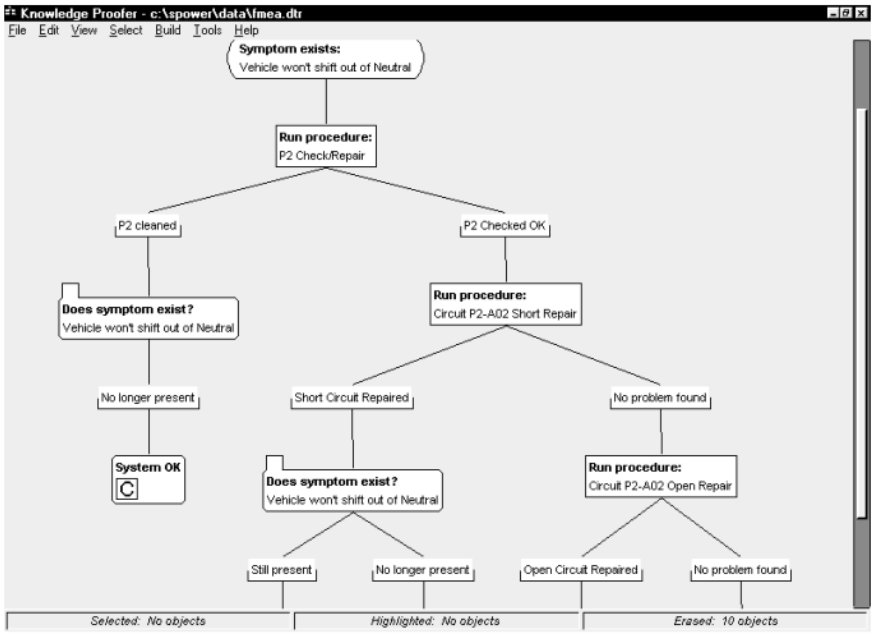

Figure 8: Diagnostic Logic Tree (Barkai, 1999)

While the diagnostic FMEA and diagnostic expert tool improved the percentage in which service technicians successfully troubleshot and repaired problems, several limitations exist with using FMEA as a foundation for service analysis. Adding service and diagnostic information into the FMEA process overburdens an already difficult process.

Failure modes, effects, and diagnostic analysis (FMEDA) extends an FMEA to measure diagnostic coverage of a system. Diagnostic coverage is the probability that a failure will be automatically detected by the systems after the failure occurs. Having a measure of diagnostic capability and understanding diagnostic coverage gaps can drive better diagnostic design which improves system availability. As with the other FMEA extensions, FMEDA only shows diagnostics for known component failure modes (Goble & Brombacher, 1999), and it is a cumbersome process to apply to complex systems.

2.2.3 Reliability Centered Maintenance (RCM)

Reliability Centered Maintenance was first developed in the commercial airline industry to improve safety and reliability. Historically, aircraft maintenance plans required scheduled overhauls to meet safety and reliability goals. These overhauls were expensive, and often introduced other problems during the disassembly and reassembly process. The industry recognized a need to confirm that technicians not only "did the job right", but also that they "did the right job" (Moubray, 1997). In 1974, the US Department of Defense commissioned United Airlines to prepare a report describing their method used to create maintenance programs (Moubray, 1997). This DoD commissioned report by Nowlan and

Heap is the first known RCM publication (Nowlan & Heap, 1978). The RCM process described by Nowlan and Heap strives to identify maintenance that is actually needed instead of basing maintenance recommendations off conservative design estimates.

RCM is a comprehensive decision making process based on an FMEA. It begins with the same steps of an FMEA: identifying system functions, failure modes, and failure effects. Then a decision logic is used to create a maintenance program. These decision criteria help the analyst determine if a proactive maintenance task is worth doing and if so, when. If there is no proactive task needed, the decision tree suggests failure checking tasks to detect hidden failures, redesigns, or fix-as-fail strategies. An example of a RCM decision tree is shown below in Figure 9.

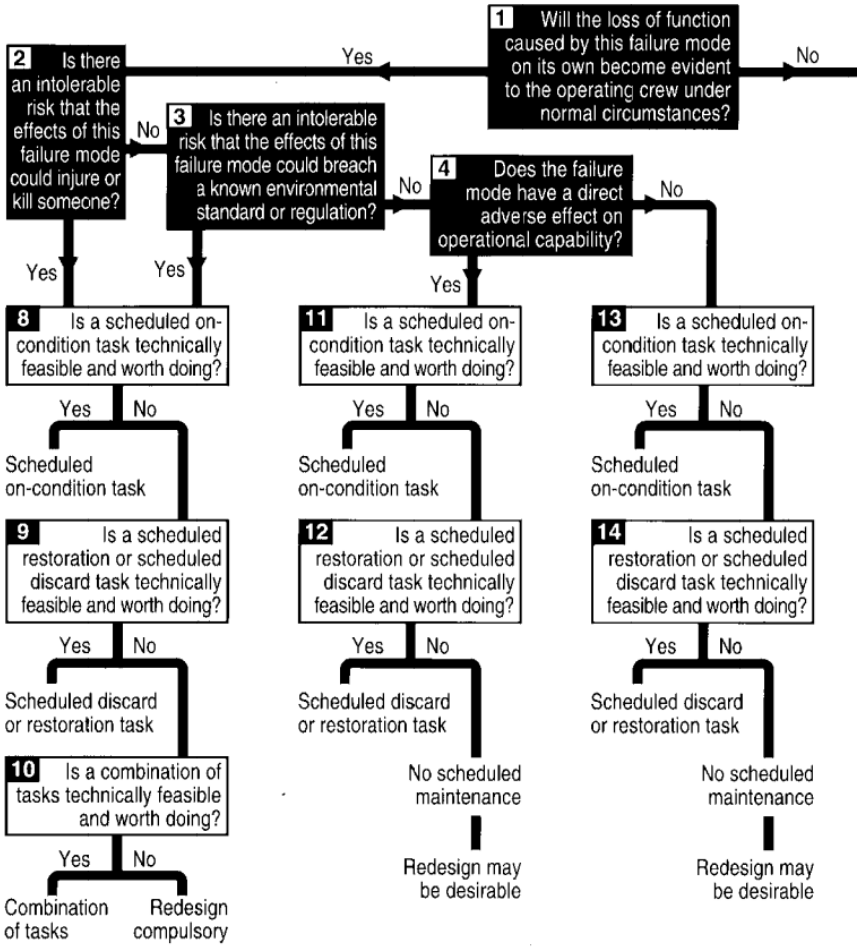

Figure 9: Excerpt of an Example RCM Decision Tree (SAE International, 2002)

RCM expands on the FMEA to include information about failure detection and confirmation and what must be done to repair a failure. There are seven basic questions that RCM answers (SAE International, 1999):

- What are the system functions?
- In what ways can the system fail to fulfill its functions (functional failures)?
- What causes each functional failure (failure modes)?
- What happens when each failure occurs (failure effects)?
- In what ways does each failure matter?
- What should be done to predict or prevent each failure (proactive tasks)?
- What should be done if a suitable proactive task cannot be found?

While RCM provides a comprehensive thought process for developing maintenance plans, its limitations are similar to other FMEA based methodologies. It focuses on known failure modes and doesn't provide a mechanism to identify unknown unknowns. RCM ignores the larger sociotechnical system, and its influences on the equipment design. RCM also leaves the human out of the analysis, and it doesn't accommodate software. Because it adds process and information to an FMEA, an RCM analysis is most likely cumbersome and time consuming to conduct and maintain.

2.3 System-Theoretic Accident Model and Processes (STAMP)

STAMP (System-Theoretic Accident Model and Processes) is an accident causality model based on systems theory. STAMP addresses emergent properties, like safety, as a control problem and consists of three key elements: safety constraints, hierarchical safety control structures, and process models. The underlying theory is that emergent properties are controlled through constraints. Undesirable emergent behavior results from insufficient control or enforcement of the constraints (Leveson, 2011). STAMP shifts the focus from "preventing failures" to "enforcing constraints on system behavior" (Young & Leveson, 2014). In this approach, failures are only one type of cause to be controlled. STAMP is powerful because it captures failures and many more non-failure causes.

The second key element of STAMP is the hierarchical control structure. Systems can be represented as different levels of abstraction, where higher levels control lower level behavior (Leveson, 2011). Each level must communicate information to the next level to control system behavior, and feedback must be received from lower levels so the correct decisions and adaptive control can be applied. The functional control structure includes individual component controls, but also includes controls needed on the interactions between components. This concept enables STAMP to capture emergent properties that are missed when individual components are analyzed separately.

Control is a broad concept, not limited to the physical system design. Controls may also include process and social controls such as employee incentives, government regulation, and defined development processes (Leveson & Thomas, 2018). Figure 10 is a generic example of a hierarchical control structure. Control actions are shown with downward arrows and feedback is shown with upward arrows. This control structure is good example of multiple levels of control that integrate both the physical process and the larger sociotechnical system.

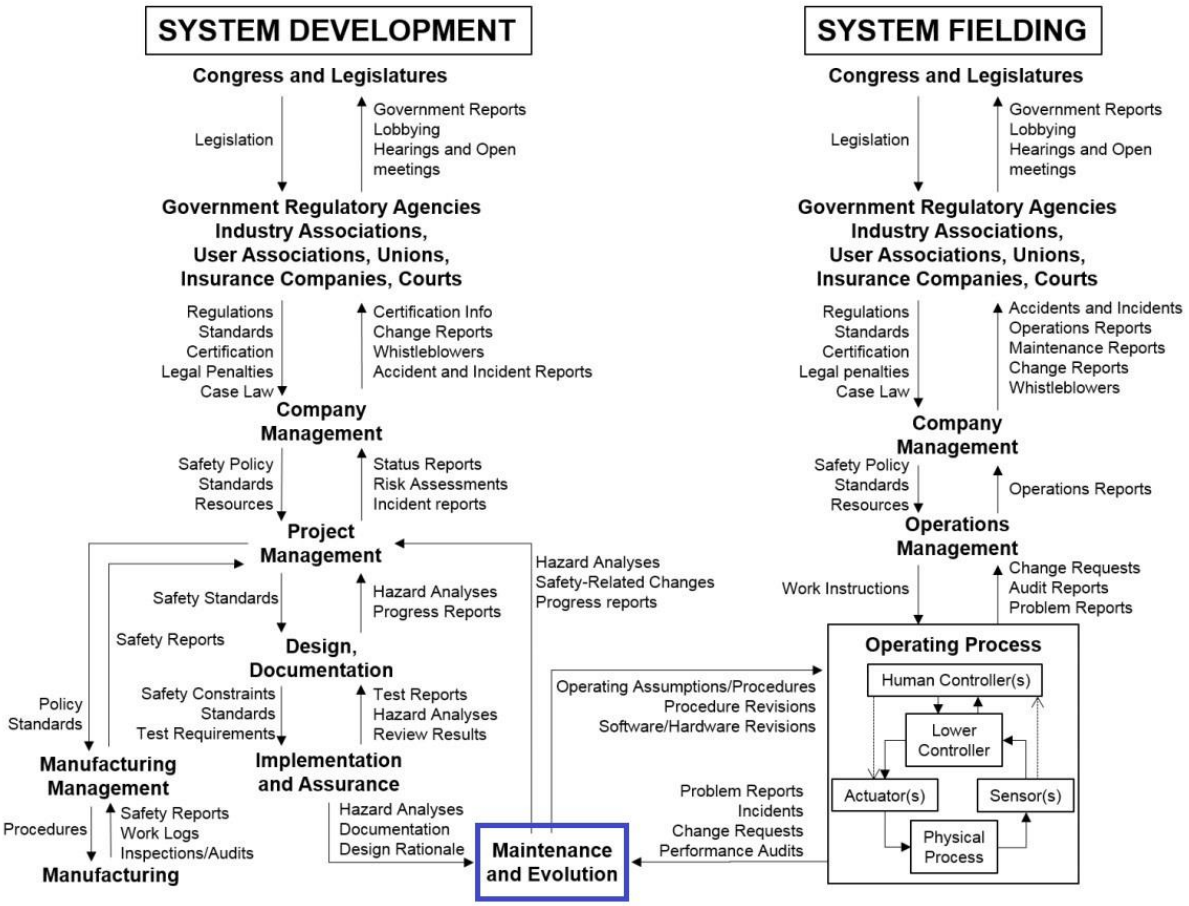

Figure 10: Example of Hierarchical Control Structure (Leveson, 2011)

It's interesting to note that this general example of a hierarchical control structure includes maintenance and evolution. System development provides controls on the operating process in the form of operating procedures, procedure revisions, and software/hardware revisions. The operating process provides feedback such as problem reports, incidents, change requests, and performance audits. This general example provides a foundation for the service control structures created for the two case studies.

The graphical control structure is key to simplifying the analysis and the system being analyzed. It allows the analyst to add detail where applicable while maintaining the higher level system perspective

(Young & Leveson, 2013). The graphical representation is easier to understand and navigate than traditional FMEA worksheets that include hundreds of line items. FMEA is a bottom up analysis, so it requires examining the low level details right away verses allowing the analyst to add details where necessary. The STAMP graphical control structure enables more efficient reviews that are often less time and resource intensive than FMEAs.

Process models are the third key concept of STAMP. To effectively control a process, a controller needs a model of the process being controlled (Leveson, 2011). The controller could be an automated electronic controller with an embedded process model or a human with a mental process model. This is a key strength of STAMP, because traditional methods often leave humans out of the analysis. For example, undesirable actions can happen when the human operator's mental model doesn't reflect reality. Excluding the operator from the analysis, misses important opportunities to prevent accidents.

2.3.1 System-Theoretic Process Analysis (STPA)

STPA is a STAMP-based hazard analysis technique developed by Leveson to identify unsafe interactions of system components, enabling "design for" safety early in the development process. STPA addresses many limitations of the traditional hazard techniques. Many comparisons of STPA and FMEA have been done, and they all indicate that STPA finds more causal factors than FMEA (Leveson & Thomas, 2018). Beyond including component failures, STPA includes non-failures like software flaws, missing design requirements, management and cultural influences, and human decision making errors. STPA enables evaluating highly complex, sociotechnical system interactions where FMEA focuses only on physical components failures. Previous comparisons between STPA and FMEA also indicate that STPA is a more efficient process, reducing time and resources required to perform the analysis and develop system safety constraints and recommendations (Leveson & Thomas, 2018).

STPA was developed to design safety into a system from the start, and it doesn't require a design to exist before it can be applied. Guiding the design from the earliest phases of development saves costly re-design when problems are found after releasing software, creating virtual models, and building physical parts. STPA can be used in early conceptual design and system architecting phases. As the design progresses, details can be added into the STPA model and analysis. High level system safety requirements are allocated into detailed design requirements, maintaining traceability throughout the process.

To effectively guide a design early in the development, methods must be capable of handling system complexity and reducing it to a level of human understanding. Traditional hazard analyses manage complexity by decomposing systems into components. This isn't effective for safety, because it

doesn't capture component interactions. STPA manages complexity through system abstraction and hierarchical models. This method captures behaviors that emerge when components interact. The analysis starts with a short, high level list. The analysis is incrementally expanded by adding details at lower levels. This layering and traceability effectively reduces complexity to a level of human understanding, and it improves confidence in the analysis completeness.

As shown in Figure 11, there are four main steps of STPA. It starts with defining the purpose including identifying system losses, hazards, and safety constraints. Next, a control structure is created to model the control actions and feedbacks that capture functional relationships and interactions. The third step includes identifying unsafe control actions (UCA) that can occur in the following four ways (Leveson, 2011):

- A control action is not provided or not followed
- An unsafe control action is provided
- A potentially safe control action is provided too early, too late, or in the wrong order
- A control action is stopped too soon or applied too long

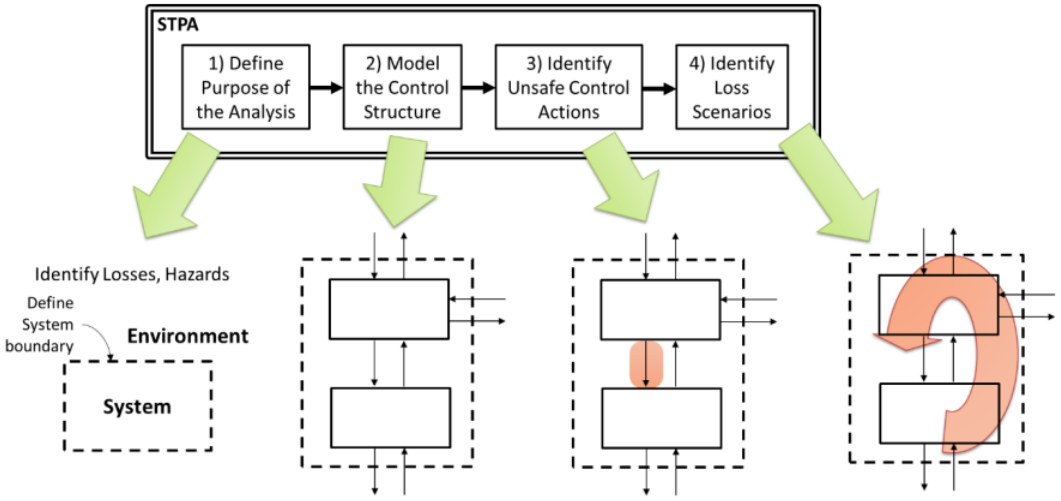

Figure 11: Overview of STPA (Leveson & Thomas, 2018)

Next the UCAs are examined to determine how the UCA could occur and identify causal factors leading to the loss. For example, this step finds missing feedbacks, inadequate process models, and conflicts that can occur when a component is controlled by multiple controllers. By evaluating the parts of the control loop and considering how the controls can change or degrade over time, the analyst can identify loss scenarios and specific constraints needed for a safe system design and management.

STPA has several advantages over traditional hazard techniques. It can be used to understand complex systems and find unknown unknowns. It can be started early in the conceptual design phases, then refined as more details are defined. STPA includes software and human controllers instead of simply decomposing the system into physical components. It handles all types of undesirable emerging behavior, whether it originates from failures, design flaws, or human interactions. Because STPA accounts for emergent behavior, it lends itself for use beyond safety and hazard analysis. Section 2.4 explores existing extensions of STPA to non-safety emergent properties.

2.3.2 Causal Analysis based on STAMP (CAST)

Leveson also developed a STAMP-based accident analysis technique called CAST (Leveson, 2011). The purpose of CAST is to learn as much as possible about past accidents so they can be prevented in the future. Accident analyses often describe events leading up to an accident, then choose one of these events as the "root cause." The events are typically considered independent, and how the root cause is selected is subjective and open to hindsight bias. Often the analysis determines blames a human and stops looking any further. When accidents are oversimplified to a few root causes or blamed on an operator, *why* the event occurred isn't deeply explored and learning opportunities are missed. Because CAST is STAMP based, it considers the whole sociotechnical system, and it doesn't focus on a single root cause. CAST helps shift an accident analysis from placing blame to learning as much as possible about why something happened.

There are five main steps of CAST, as shown in Figure 12. Similar to other STAMP-based methods, the first step includes defining the system and the system boundary, describing the losses, hazards, and system safety constraints. In addition, the events leading up the accident are explained and questions generated that need to be answered to understand why the events happened. Step one also includes examining the physical system to figure out its contribution to the loss event and to determine why the physical controls in place didn't prevent the hazard (Leveson, 2011).

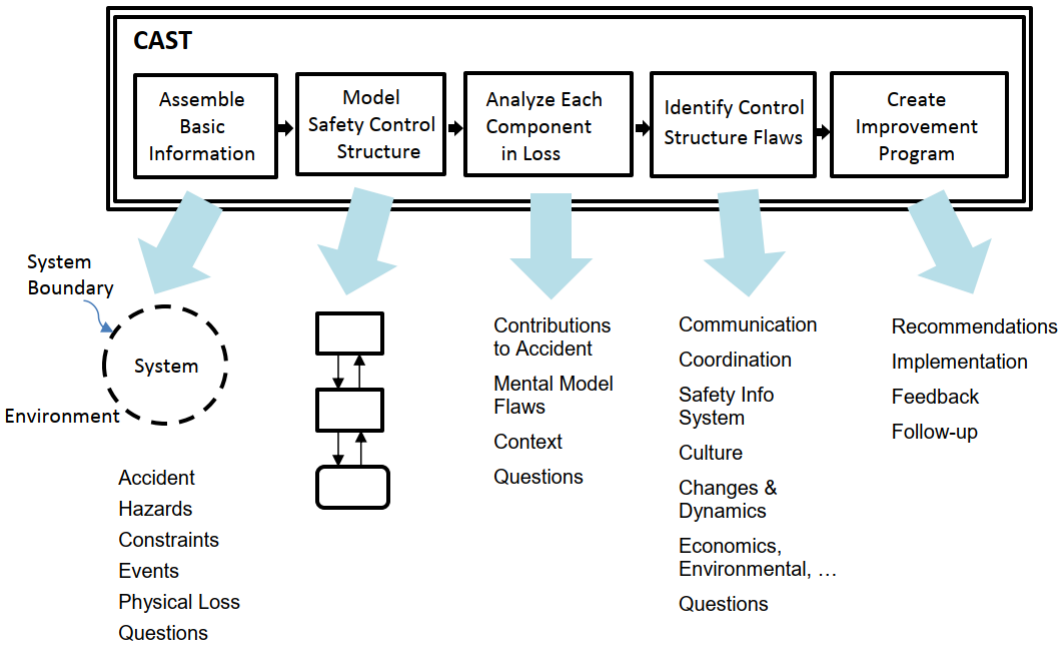

Figure 12: Overview of CAST (Leveson, 2019)

After gathering basic information about the event, the rest of the analysis finds weaknesses in the safety control structure and recommends how to strengthen it to prevent future accidents. This starts by modeling the safety control structure, including roles, responsibilities, controls, and feedback. Starting at the bottom then moving up the hierarchical control structure, each element is examined to understand how and why it contributed to the accident. This step identifies mental model flaws and any contextual factors that explain the behavior of each component. Next, flaws in the control structure as a whole are identified. This step focuses on systemic factors that affect multiple elements in the control structure, such as coordination and communication contributors. Lastly, change recommendations are generated to prevent a future loss.

As with other STAMP-based methodologies, CAST has many advantages over traditional techniques. CAST identifies systemic contributions verses focusing on physical failures and human errors. CAST captures what happened and why, instead of who and why. This shifts the analysis from accusing to explaining. As presented by Leveson, "blame is the enemy of safety" (Leveson, 2011). Analyses that place blame restrict information sharing and limit learning from past events. By taking a system approach to human behavior and avoiding blame, CAST identifies more causal factors and generates more recommendations on how to prevent the future losses.

2.4 STPA Extensions

Although STAMP was originally created for system safety, its foundation in systems theory lends itself to other emergent properties. Key to this flexibility is the broad definition of a loss. Instead of restricting losses to loss of human life or injury, a loss can be anything that "is unacceptable to the stakeholders" (Leveson & Thomas, 2018). By identifying losses for the specific purpose of the analysis, STAMP techniques can be applied to any emergent property. This section explores a few selected STPA extensions to frame how system serviceability could be another application.

Probably the most well explored extension of STPA is the extension to security, STPA-Sec. Young and Leveson laid a foundation for applying STPA to cybersecurity, pointing out that safety and security have a common goal of mission assurance (Young & Leveson, 2014). Traditionally, safety focuses on "unintentional actions by benevolent actors" and security focuses on "intentional actions by malevolent actors." However, differentiating whether the action was unintentional or intentional is difficult. By re-framing the problem to identify and control vulnerabilities, the analysis focuses on what the system can control.

Integrating security and safety into a simultaneous STPA is straightforward, and the four basic STPA steps apply. In step one when defining the purpose of the analysis, security is identified as an object of the analysis. Because safety and security have a common goal of mission assurance, losses, system-level hazards, and safety constraints are typically common between safety and security. Step two of modeling the control structure is also the same. While step three, identifying UCAs, is the same, reframing the four types of potential unsafe/unsecure control actions to include security-facing language may be helpful. Instead of only considering what can lead to a hazard, consider what UCAs can lead to a hazard or *exploit a vulnerability* (Young & Leveson, 2013). When identifying loss scenarios, one additional possibility is explored: identify if and how the control action or feedback "could be injected, spoofed, tampered, intercepted, or disclosed by an adversary" (Leveson & Thomas, 2018). In this way, STPA can be extended to cybersecurity.

Ball demonstrated a producibility analysis based on STPA (Ball, 2015). Producibility is the ability of product development and operation systems to meet cost, schedule, quality, and performance needs. It is an important emergent property of any product development system. Ball extended STPA to producibility in a case study of a complex product development program in a large Aerospace company. Ball's research is one demonstration of how the first STPA step, "define the purpose of the analysis", is important to execute an STPA on other emergent properties. For the producibility analysis, Ball defined a loss as anything unacceptable to the product development organization. For example, loss of quality, loss

of performance, exceedance of cost targets, and missed schedule commitments were all considered as producibility losses. While different from safety losses, they still comply to Leveson's definition of a loss: "A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders. (Leveson, 2011)."

Ball's producibility control structure model focused on the product development system's ability to assess producibility governance. The unproducible control actions (UCA) were evaluated using the standard four sources of inadequate control: not provided, provided, incorrect timing, and stopped too soon/applied too long. Then scenarios were explored to determine casual factors. Overall, Ball's research showed that the process between a safety STPA and a producibility STPA is the same.

STPA has also been applied to quality. Goerges successfully applied STPA to a quality hazard analysis in two case studies (Goerges, 2013). One case study focused on a new product design and one case study investigated a known warranty design issue. In both studies, Goerges determined that STPA based quality analysis identified more causal factors than FMEA and Fault Tree Analysis. In the second case study, Goerges pointed out that while Fault Tree Analysis found the design error, it did not identify problems with the design process that led to the design error. To adapt STPA to quality, the primary loss was identified as the "inability to meet emissions." Goerges suggests different terminology when applying STPA to quality. For example, "undesired system state" instead of "hazard" and "inadequate control actions" instead of "unsafe control actions." Goerges also explored expanded causal factor guidewords. As seen in the other extensions, the overall STPA process was demonstrated to be the same whether analyzing safety or quality.

Testing has been explored as another STPA extension. Montes demonstrated using STPA to inform product testing (Montes, 2016). One interesting aspect of Monte's research is the addition of system testing into Leveson's general example of a hierarchical control structure, Figure 13. Monte highlights that traceable product documentation must be communicated between product development stages and between the design and test teams. Adding a testing stage to the organizational control structure visually shows the information flowing between the stages and the "test-specific safety communications" needed during product evaluation.

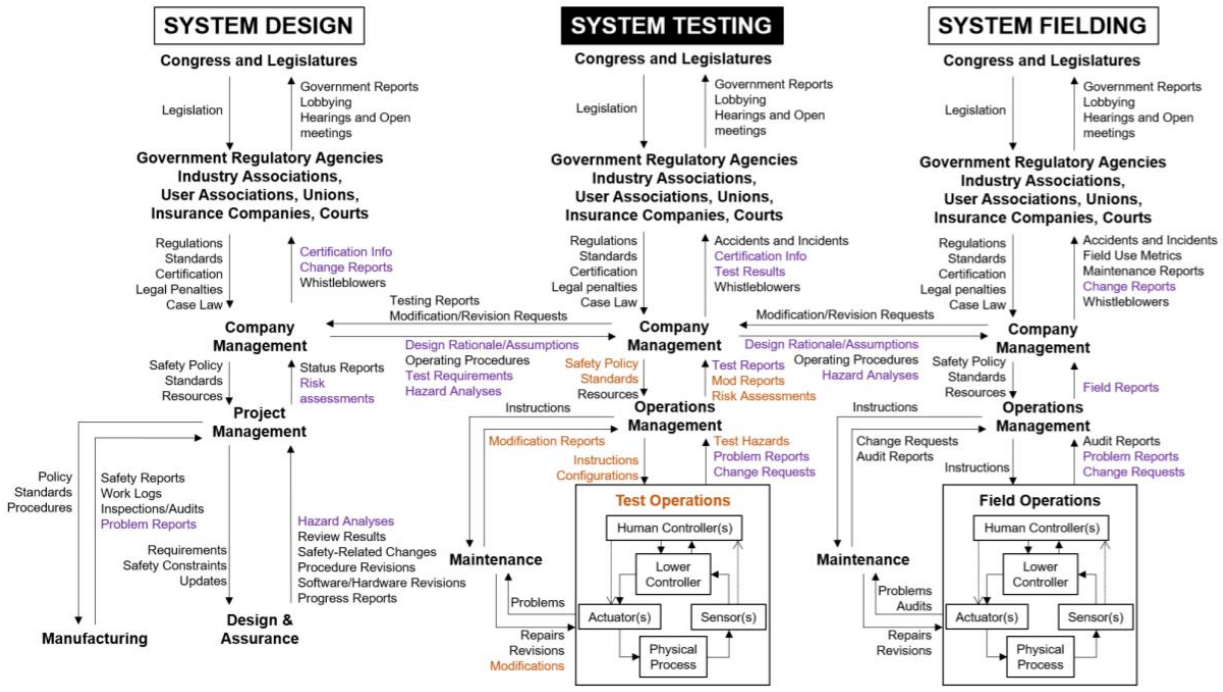

Figure 13: System testing added to heirarchical control structure (Montes, 2016)

This thesis references the general hierarchical control structures developed by Leveson, Figure 10, and expanded to testing by Monte, Figure 13. Both control structures define maintenance as a control element of the physical system operating process. Maintenance controls include operating procedures, procedure updates, and software/hardware updates. Feedback required from the operating process are problem reports, incidents, and change requests. These maintenance controls and feedback are considered and incorporated into a service hierarchical control study as part of the first case study.

Monte highlights that maintenance and operations are incorporated in both the test and field stages. This is an important concept to further explore in this thesis. If product testing operates and services the product during system testing, product test may have a key role in evaluating product serviceability. The first case study will expand on this concept.

Building on other STPA extensions, the idea of adapting terminology for service was considered by the author. Some of the STAMP terminology, such as “accident” and “hazard”, have safety connotations in the English language, and they could cause confusion for the team applying STPA to serviceability. However, after researching STPA and STPA extensions, the author suggests reusing Leveson’s STAMP terminology as much as possible. These terms are already widely understood and accepted by STAMP practitioners. Aligned terminology enables cohesiveness between various uses of STPA and encourages a common STAMP language. One minor adaption that will be explored is substituting “unserviceable” for

"unsafe." This allows reusing the "UCA" acronym, aligns with Leveson's definition, and enables easy adaptation to other emergent properties.

Table 1: STAMP Terminology

STAMP Term	**STAMP Definition**	**Proposed Service STAMP Term**
Loss	A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders. (Leveson, 2011)	Loss
Accident	An accident is an unplanned and undesired loss event. (Leveson, 2011)	Loss Event
Hazard	A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. (Leveson & Thomas, 2018)	Hazard
Unsafe Control Action	An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard. (Leveson & Thomas, 2018)	Unserviceable Control Action

This research contributes to STAMP methods by demonstrating its application to an unexplored emergent property, serviceability. No applications of STPA or CAST to repair, maintenance, or diagnostics were found in the literature review. While other non-safety emergent properties have been explored such as Ball's producibility application, Goerges's quality application, and Monte's testing application, none explored serviceability.

Another gap in the current research is that the other non-safety STAMP applications focused heavily on the organizational and process control structure, such as the design process. They did not deeply analyze the physical process control system and physical process. Case study two in this thesis focuses on using STPA to generate detailed software and hardware design requirements to ensure serviceability of a future system. This thesis explores the whole hierarchical control system in the first case study using CAST and focuses on the physical process control structure in the second case study using STPA.

Both case studies in this thesis are founded in Leveson's broad definition of a loss, see Table 1. Leveson's definition enables extending STAMP to serviceability. For example, a serviceability loss may be unplanned downtime due to inadequate serviceability. Customers expect equipment to work when it's

needed, and unplanned downtime is unacceptable to the customer as a stakeholder. Founded in STAMP and building on other non-safety STAMP explorations, this research demonstrates STAMP's wide potential to influence industry approaches for generating and enforcing system constraints.

3 Case Study 1: Applying Diagnostic CAST to Existing Issue

The purpose of this case study is to explore how STAMP can be applied to serviceability by analyzing a current production diagnostic issue using CAST. The analysis identifies why existing system controls did not effectively prevent the diagnostic issue. It then recommends potential changes to the product and the development process to address the issue and avoid similar losses in the future. This section reveals that CAST can be extended to serviceability.

The case study leverages an existing diagnostic issue. The case study information was gathered through data from the manufacturer, interviews, and the author's experience. Analysis details cannot be disclosed due to the proprietary nature of the content. Therefore, diagnostic loss events, system specific details, and system contributions to the hazards are generalized.

This section steps through the CAST analysis process and captures findings, questions, and recommendations. The analysis is incrementally expanded by adding details at each step, while tracing relationships throughout the process. Identification codes were created and used to enable this traceability. Figure 14 is a generic example showing how CAST analysis elements relate to each other and incrementally drive more details into the review.

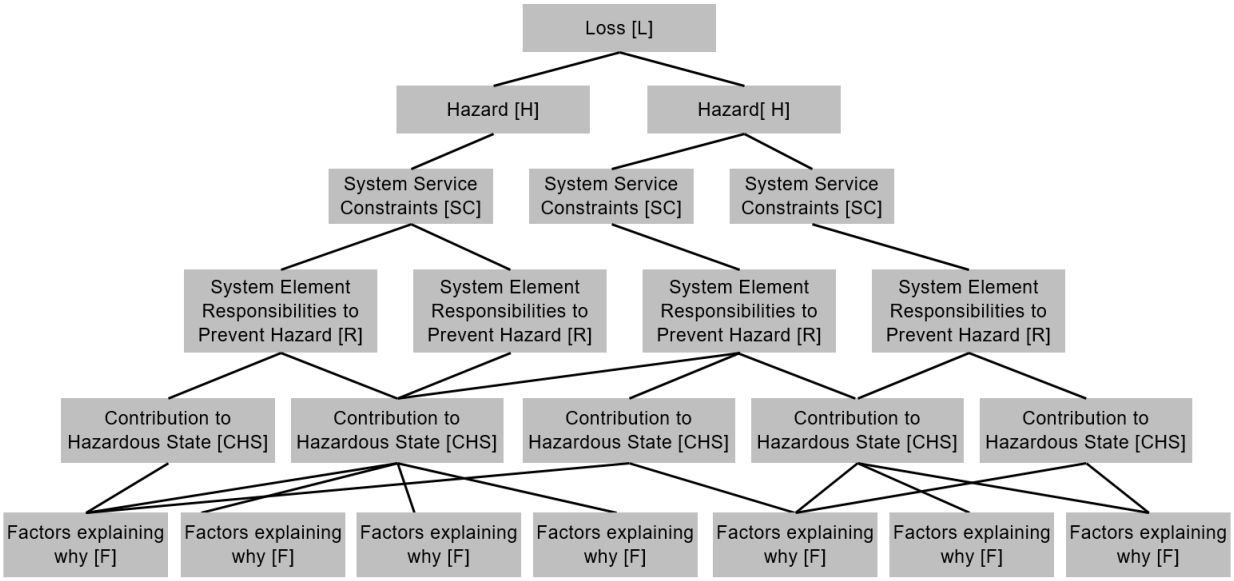

Figure 14: Relationships and traceability between elements of a CAST analysis

In the spirit of traceability and completeness, questions are documented as they were generated. After the analysis was completed, these questions were reviewed and traced to the answers found. If the analysis answered the question, the reference to the answer is captured after the question. For example, *(Question: Why did the order of diagnostic steps vary significantly? [ST.CHS-2, PS.CHS-4]).* In this

example, the answers are found in the contributions to the hazardous state [ST.CHS-2 and PS.CHS-4] and the associated factors explaining why.

3.1 Diagnostic Loss Event Summary

A difficult to diagnose machine condition is low transmission supply pressure. When low supply pressure is detected on start-up, a low supply pressure Diagnostic Trouble Code (DTC) triggered. DTCs are service alarms that indicate a problem and identify the service action needed. When supply pressure is low, the machine is automatically prevented from moving and is locked in park. With the machine unable to move, diagnostics are critical to getting the machine back up and running quickly. However, this DTC can be triggered by a large number of potential problems. The system is unable to isolate the problem and pin point the repair required, so it's up to the service technician to perform manual troubleshooting checks.

When the low supply pressure DTC occurs, customers and service technicians struggle to identify the repair required. The average labor time to resolve the low pressure DTC is four times longer than average labor times. Many TAC (Technical Assistance Center) cases exist about low supply pressure, which indicates that dealers are heavily reliant on escalated support to troubleshoot the condition. Data also indicates that many technicians skip detailed diagnostic checks. Instead they rely on "swapnostics," where parts are swapped into the system until the problem is resolved. Swapnostics leads to functioning parts being replaced, driving up costs for the customer and warranty costs. Better controls are needed to enable system diagnostics.

3.2 System Background

Several years ago, a new ground drive transmission (AST) and a new auxiliary drive system (PST) were introduced. Both transmission systems incorporated electro-hydraulic valves to engage and disengage various functions. This drove significant changes to the electrical, hydraulic, and drive systems.

To support the new gearcases, the main gearcase (MG) hydraulic circuit evolved over time. The existing MG hydraulic system had been in production for many years and was originally designed to support the steering and MG functions. To limit legacy system design changes, the AST and PST functions were added to the MG circuit. This architecture enabled reusing and sharing components, like the reservoir and oil cooler. Figure 15 is a high level view of how the hydraulic system architecture evolved over time, incorporating additional functions into a legacy system.

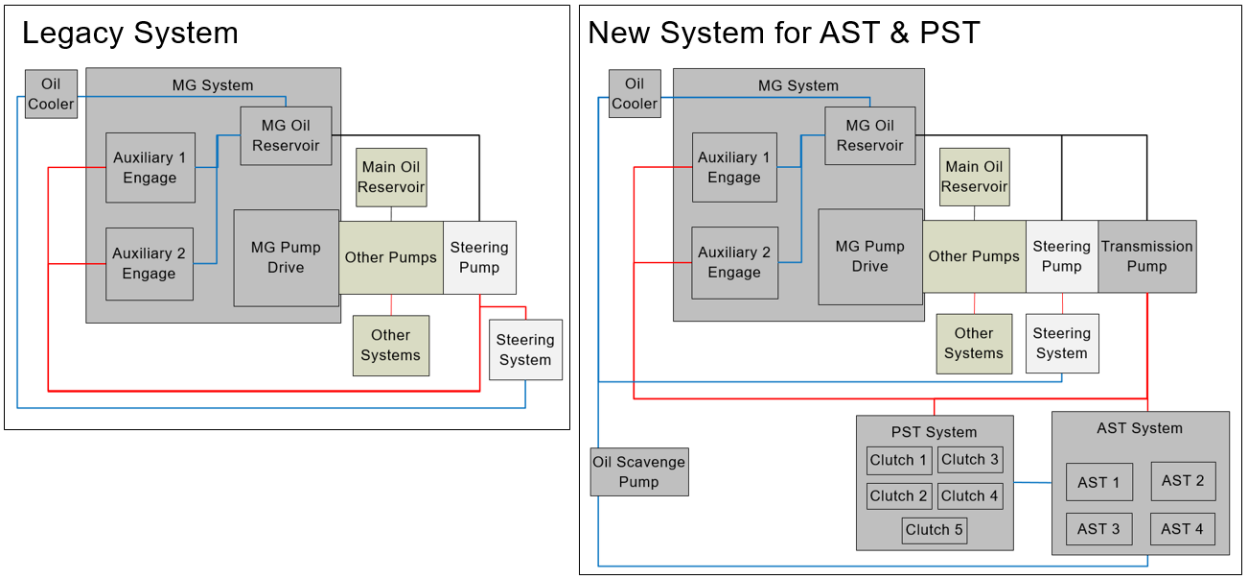

Figure 15: System Design Evolution

The new design changed a mature, relatively simple system into a complex system with additional functions and interfaces. The self-diagnostic capability of the system did not keep pace with the complexity. When the low pressure DTC occurred, there were over thirty possible repair actions that could resolve the condition. This required the service technician to perform many manual troubleshooting checks to determine the correct repair.

3.3 CAST Step 1: Assemble Basic Information

3.3.1 Define System and Boundary

The goal of the analysis is to determine why low supply pressure is difficult to diagnose and to identify recommendations to the physical process, the system operation process, and the system development process to prevent inadequate diagnostics in future systems. The development process includes system design, verification, and implementation. The operations process includes the physical system as well as the operator, service technician, and support of the equipment post-production.

The physical system analyzed is the regulated supply pressure system that engages and disengages the AST functions, PST clutches, auxiliary 1, and auxiliary 2. As shown in Figure 16, the supply pressure system, including DTC software and the physical components, are in scope. Detailed analysis of the equipment retailer, service shops, farm operation, and industry standards and regulations are out of scope. Even though they are out of scope, the service shop/dealer and the farm operation are included in the

control structure and element analysis. Many unanswered questions were generated for these out of scope elements that could enable a more detailed analysis on these elements in future studies.

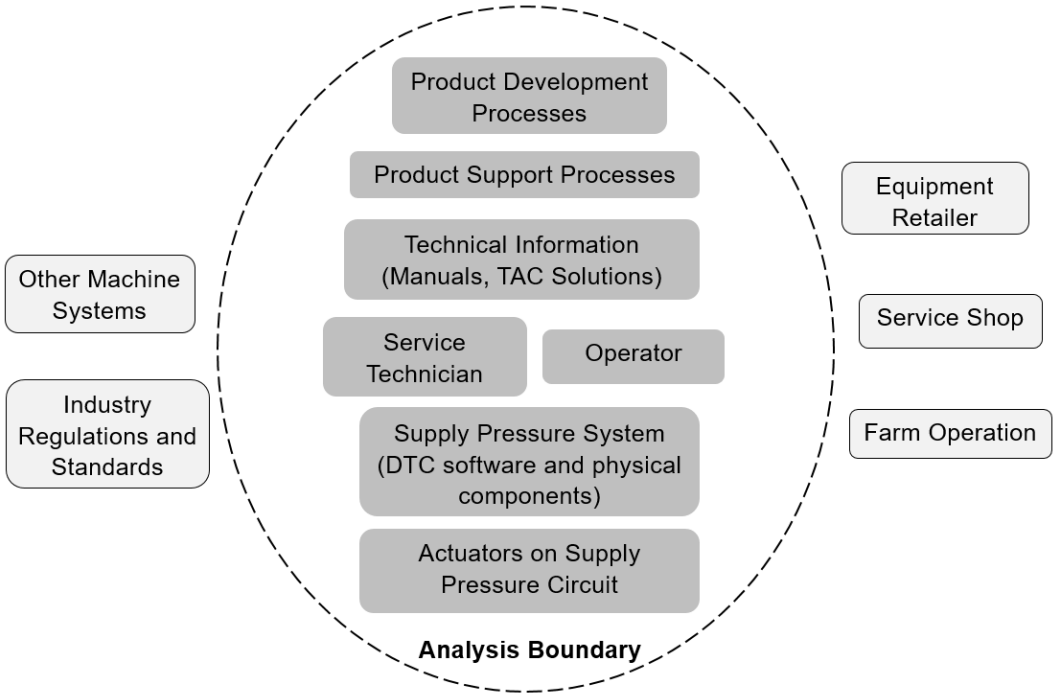

Figure 16: CAST Boundary

3.3.2 Events & Questions

This section describes what happened and captures questions that need to be answered to explain why the events occurred. The diagnostic loss "event" isn't a single event, it is a collection of events related to the system being difficult to troubleshoot. Therefore, the event description is a summary of information gathered, and it highlights recurring events. An attempt was made to avoid blame and hindsight bias.

Common Operator Actions: Listed below are common observed symptoms and operator actions associated with the low supply pressure on startup DTC.

1. Low supply pressure DTC occurs every machine startup. Operator cycles the key and restarts the engine, but the DTC persists. Operator calls a service technician.
2. Low supply pressure DTC occurs along with other DTCs at the same time. Operator cycles the key and restarts the engine, but the DTCs persist. Operator calls a service technician.
3. Low supply pressure DTC occurs when the machine is started in the morning. Operator cycles the key and restarts the engine, and the DTC goes away. Besides the DTC alarm, the machine operates as

expected. DTC may reoccur after shutting down for an extended period of time. *(Question: Why does DTC go away instead of coming up every time the machine is started? [PP.CHS-2]. What is the software process model for triggering and recovering DTC? Does it account for environmental conditions? [PCU.CHS-1])*

Common Service Technician Actions: Listed below is a collection of various service technician actions taken to resolve the low supply pressure on startup DTC. These include troubleshooting steps and repair actions taken.

The order of these steps varies significantly across cases. (*Question: Why does the order of diagnostic steps vary significantly? [ST.CHS-2, PS.CHS-4] Which of these checks are included in the diagnostic procedures? If not included, why did the service technician do them? [See below]*).

In some cases, the service technician did a few of the diagnostic steps on their own, but they called TAC before finishing the diagnostic procedure described in the technical manual (TM). In some cases, the service technician followed the full diagnostic procedure, but the code still existed so they called TAC. (*Question: Why did diagnostic procedure not identify repair required? [PS.CHS-3]).*

1. Replace the sensors and the code goes away. *(Question: Why replace the sensors without doing any other troubleshooting first? [PP.F-8])*
2. Swap the pressure sensors, but code still exists. Remove sensor, install a diagnostic receptacle fitting, and manually check pressure with a gauge. Pressure is within published specification. Replace sensor with new. Code still exists. Check diagnostic addresses and find pressures are out of specification. Troubleshoot wiring circuit and repair harness.
3. Replace the sensors, but code still exists. Manually check pressure and pressures are within specification. Check diagnostic addresses, pressures are within specification. Call TAC. *(Question: Why call TAC before completing the diagnostic procedure in the manual? [ST.CHS-4])*
4. Check Diagnostic Addresses, replace the sensors, update all software. Swap or replace electrical control unit. *(Question: Why update software and replace the control unit when this isn't included in the diagnostic procedures? [ST.F-11, ST.F-12])*. Call TAC.
5. Manually check supply pressure and it is below specification in technical manual. Troubleshoot the hydraulic system. (*Question: Does the pressure specification in the technical manual (TM) match the threshold in the DTC software process model? [Yes] Does the pressure specification account for noise and other normal operating conditions like temperature? [PCU-CHS-1]*).

Listed below is a collection of various troubleshooting checks and repairs tried by technicians or recommended by technical support specialists after the pressure was manually checked and found below specification:

a. Replace valve A
b. Replace valve B. (*Question: Why replace valve B before verifying a valve problem? [ST.F-4])*
c. Adjust valve B to a higher setting
d. Remove and check valve C for damage and debris
e. Adjust valve C to a higher setting
f. Remove and check AST valves for damage and debris. (*Question: Why not verify pressures before removing and checking valves? [PP.CHS-4])*
g. Monitor PST clutch pressure diagnostic addresses while shifting through the speeds. If low in only a specific gear, check and repair clutch. Manually check pressure at PST clutches.
h. Disconnect supply pressure hose to PST to isolate PST from the system. If DTC goes away, this indicates a problem with the PST system.
i. Check MG oil level (*Question: Why isn't this always the first thing checked? [OP.CHS-1] Why isn't AST oil level checked too? [PP.CHS-3])*
j. Mistakenly check main hydraulic oil level instead of the MG oil level. *(Question: Why is wrong oil level checked? [ST.CHS-1])*
k. Manually check MG lube pressure. If it's low, adjust the MG lube pressure valve to increase pressure. *(Question: Why check MG lube pressure when DTC indicates low supply pressure? [ST.F-12])*
l. Disconnect supply pump suction hose and check suction screen for damage or debris
m. Disconnect scavenge pump suction hose and check suction screen for damage or debris
n. Remove scavenge pump, disassemble and check shaft for damage. Replace scavenge pump. (*Question: Why are pressure and flow not manually checked before disassembling or replacing the pump? [PP.CHS-5, ST.F-4])*
o. Replace supply pump. (*Question: Why are pressure and flow not manually checked before disassembling or replacing the pump? [PP.CHS-5, ST.F-4])*
p. Check oil filter for damage and excess debris. Replace if needed. If there is excess debris, locate the source of the debris. If debris found, repair as needed and flush hydraulic system to remove contamination.
q. Check for external leaks. Repair and replace plumbing and seals as needed. (*Question: Why did leak occur? [Unknown])*

r. Check for other DTCs or observed symptoms that could indicate hydraulic system problem.

Design Changes and Technical Information Updates: Below is a summary of design changes and technical information updates related to the supply pressure system.

1. Updated DTC software to account for environmental conditions and system interactions. (*Question: Why wasn't DTC design flaw detected prior to production [PT.CHS-2]? Why were system interactions and environmental conditions missed? [PP.F-7, PD.F-3]*)
2. Published a TAC solution:

   The solution describes a troubleshooting procedure to follow when a machine is experiencing symptoms of a failed pressure sensor. (*Question: Why are in-spec sensors being replaced [PP.F-8]? Does TM diagnostic procedure match the following procedure [No]? If not, why [ST.F-9]?*). The pressure sensor diagnostic procedure is described as:

   a. Warm hydraulic oil to a specified temperature range.
   b. Check and record supply pressure diagnostic addresses (DA).
   c. Manually measure oil pressure with a gauge.
   d. Compare DA and gauge pressures to specification. Specifications included in the solution.
   e. Measure sensor supply voltage and check for power, shorts, and open circuit.
   f. Visually inspect sensor and harness connectors for damaged pins and corrosion.
   g. After all these steps, replace the sensor and report the issue to TAC.
3. New sensors implemented.
4. Published a TAC solution:

   The solution describes the following procedure to follow when low supply pressure is detected:

   a. Disconnect sensor from harness
   b. Visually inspect the sensor and harness
   c. Reconnect sensors
   d. Replace sensors if DTCs are still active (*Question: Why not reference the same diagnostic procedure from previous TAC solution before replacing sensor? [Unknown, see ST.F-9])*
5. Published a TAC solution:

   The solution indicates to follow the diagnostic steps in the technical manual. If steps do not resolve the issue, proceed with manually checking the PST clutch pressures. If pressures are below specification, check valves and clutches for damage and debris. (*Question: Why did diagnostic procedure miss checking clutch pressures? [PS.CHS-4]*).

3.3.3 Losses and Hazards

Three important losses occurred in this diagnostic loss event:

- Unplanned downtime due to inadequate serviceability (L-1)
- Financial losses incurred through warranty costs (L-2)
- Customer dissatisfied (L-3)

Several different hazards led to these losses and are summarized below in Table 2. The system service constraints that must be met to prevent the hazards are also identified. As shown in Figure 14, each hazard is traced to the applicable losses and each system constraint is traced to the applicable hazards. These losses and hazards are specific to this diagnostic event, but they could also apply to other service analyses. Thinking of diagnostics as a control problem identifies two key hazards where the system drives undesired operator or service technician behavior: operator takes the wrong problem mitigation or ignores the alarm, service technician does the wrong repair.

A key service hazard is a technician doing the wrong repair (H-2). When a technician does the wrong repair, good parts may be replaced. This drives up cost for the customer and for the manufacturer if the equipment is still under warranty (L-2). Doing the wrong repair also contributes to unacceptable repair times. After completing the wrong repair, the problem is not resolved. Then the technician does additional troubleshooting, possibly orders and waits for new parts, then attempts the repair again. All this time the machine is unavailable, causing downtime and customer dissatisfaction (L-1, L-3).

An important system constraint is that the service technician must do the correct repair. This constraint is broken down into a few different constraints. This includes constraints for the product, such as the machine must pinpoint the repair required (SC-5). This also includes constrains for product support, such as troubleshooting procedures must identify the correct repair required (SC-6).

Table 2: CAST Hazards and System Constraints

Hazard ID	Hazard	Constraint ID	System Service Constraint
H-1	Operator takes the wrong action to mitigate the problem or ignores a service alarm (L-1, L-3)	SC-1	Machine must detect problems (H-1, H-2)
		SC-2	Machine must decide the operator action required (H-1)
		SC-3	Diagnostic information must clearly communicate desired operator action (H-1)
		SC-4	Machine must prevent operator alarm fatigue (H-1)
H-2	Service technician does the wrong repair (L-1, L-2, L-3)	SC-5	Machine must pin point the correct repair required (H-2, H-4)
		SC-6	If machine is unable to pin point the repair required, troubleshooting procedures must identify the correct repair required (H-2, H-4)
		SC-7	Adequate diagnostic check points must be provided (H-2, H-4)
		SC-8	Diagnostic procedures must clearly communicate desired service technician actions (H-2, H-4)
H-3	Machine falsely indicates a problem (L-1, L-2, L-3)	SC-9	Machine must positively identify problems (H-1, H-2, H-3)
H-4	Repair & troubleshooting time exceeds <X> minutes (L-1, L-2, L-3)	SC-10	Repair & troubleshooting time must not exceed <X> minutes (H-4)
		SC-11	Adequate access to perform diagnostic and repair tasks must be provided (H-2, H-4)

3.4 CAST Step 2: Model the Control Structure

This section describes the service control structure to prevent serviceability hazards. As discussed, CAST is based on the theory that losses are control problems, not failure problems (Leveson, 2019). When hazards occur, it's because the controls and control structure in place to prevent the hazard were not effective. Understanding the existing controls and control structure is a critical step in all STAMP based analyses. This section starts with a high level generic service control structure, then refines and expands the model adding details specific to the supply pressure diagnostic loss event. Generic and specific diagnostic responsibilities are also identified and explored in this section.

The general sociotechnical service control structure is shown in Figure 17. There are two main control structures involved with service: system development and system operation. Serviceability involves both designing serviceability into the equipment and supporting the equipment post-production. Analyzing product serviceability requires considering pre-production and post-production controls.

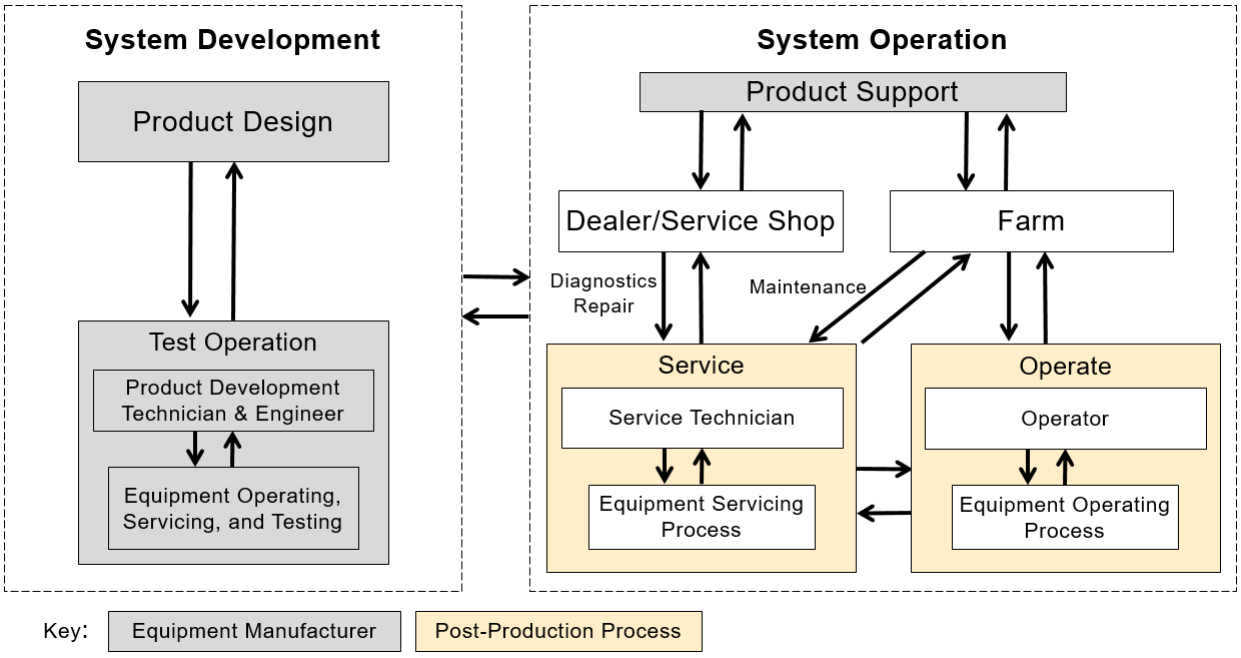

Figure 17: High Level Service Control Structure, General

During system development, key elements involved in design for serviceability include product design and product test. Testing is called out separately because when problems occur during testing, the product development team must diagnose and repair the equipment. In this way, they have a similar experience as the service technician that works with the equipment post-production. The product development test team is unique in that they not only test the equipment, but they operate it and service it as well.

During system operation, there are two processes being controlled: servicing the equipment and operating the equipment. The farm is responsible for field operation and equipment maintenance. A dealer or service shop is responsible for equipment service, focusing on diagnostics and repair. In reality the service shop may be an equipment retailer, a third-party service shop, or a part of the farming operation. Additionally, some farming operations do their own maintenance, and some hire it out to a service shop. For the purpose of this analysis, whether the service shop is independent or part of the farming operation and whether the farming operation controls the maintenance process or hires it out is left generic. The key distinction is that maintenance is a customer task, while repair and diagnostics are service technician tasks. Who employs the service technician or the maintainer is not important to this analysis.

After modeling the high level structure, details were added and specific controls identified applicable to the diagnostics loss event. The control structure shown in Figure 18 represents the controls and control structure in place to prevent this loss event. This is the final control structure after completing the CAST analysis. Many iterations occurred through the analysis as system understanding evolved. Identification codes for each system element are included in parenthesis behind the element name. For example, OP is the identification for Operator. These ID's are used throughout the analysis to enable traceability.

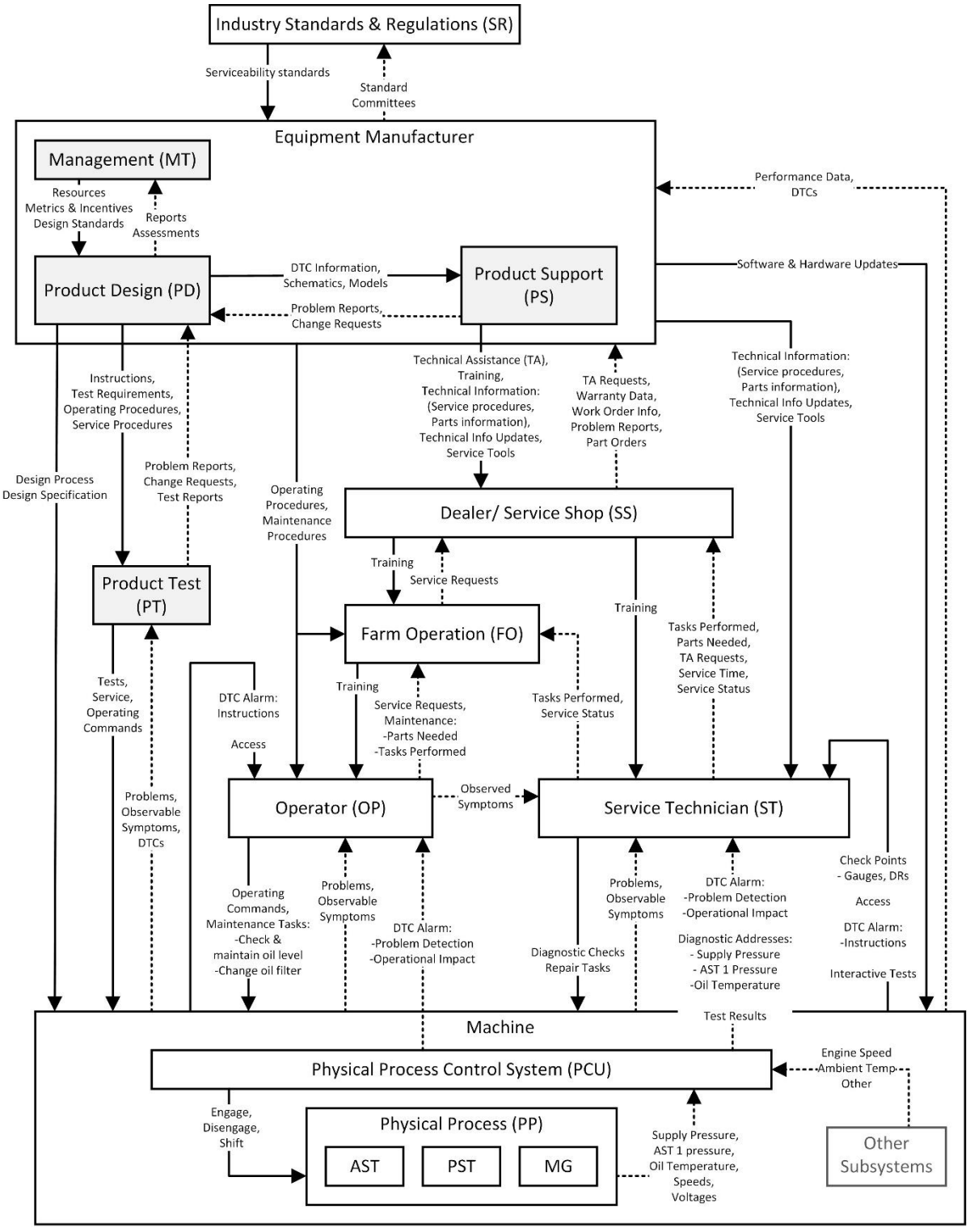

Figure 18: Service Control Structure Specific to Diagnostic Loss Event

The control structure is organized where the controlling element is shown above the process it's controlling. Starting at the top, industry serviceability standards and service related regulations, such as SAE J817, guide decisions made by the equipment manufacturer. Product development controls the equipment serviceability through the design process and the design requirements. Product design guides product test by providing instructions, test requirements, operating procedures, and service procedures. The other important role of the equipment manufacturer is to support the product post-production. When problems occur, the service technician does the troubleshooting and repair tasks. When they are unable to fix the problem, they escalate the problem through the technical assistance center (TAC). Service instructions provided by TAC are a key control guiding service technician actions. Other important product support controls include equipment software and hardware updates, operator and technician training, technical information like operating procedures, service procedures, parts information, and diagnostics aids provided through service tools.

The equipment provides serviceability controls to the operator and the service technician in the form of Diagnostic Trouble Codes (DTCs). Interestingly, DTCs have a control and a feedback element. DTC alarms that alert the operator to a problem and indicate the impact to the operation are feedbacks. Problem mitigation instructions communicated through a DTC are controls. DTC Instructions can be operation focused, such as slow down or turn off the system. They can also be service focused, such as check oil level, replace filter, or troubleshoot and repair the gearcase. Equipment service controls also include diagnostic check points such as diagnostic receptacles (DR) and access to the service points.

After modeling the control structure a few key insights stand out. First, there are multiple sources of controls on the humans in the system, both the operator and the service technician. Whenever there are multiple sources of control, conflicts can arise. If the control information doesn't match or conflicts, the person may choose to follow the "wrong" control. The operator receives operating and maintenance procedures from the manufacturer, training from the farm operation, and problem mitigation instructions from DTCs. The service technician receives technical information like service procedures and parts information from the manufacturer, training from the service shop, and problem mitigation instructions from DTCs. To compound the potential for conflicts the service technician receives service information in multiple forms: technician manuals, technical assistance center (TAC) solutions and live help, on board service tools, off board service tools, and DTCs.

Another early insight from the control structure is a potentially insufficient feedback loop to control the effectiveness a key diagnostic control. *(Question: Is feedback sufficient to understand if control is effective? [PS.F-7]).*

3.4.1 System Responsibilities

This section explores the serviceability related responsibilities of each system element. General responsibilities that can be referenced in future serviceability analyses and specific responsibilities applicable to this loss event are identified. The specific responsibilities are carried forward in the analysis, used to analyze each component's contribution to the hazard.

Consider the service technician as an example. A service technician's responsibilities include diagnosing problems, requesting the parts needed for repair, repairing the equipment, and verifying the repair. In this specific loss event, the service technician did not follow the diagnostic procedures. This was an unfulfilled responsibility that contributed to wrong parts being replaced.

This section summarizes responsibilities for a few of the key system elements. Responsibilities for the remaining elements are listed in the CAST Details Appendix.

Table 3: Service Responsibilities - Physical Process Control System (PCU)

General Responsibilities	**Specific**
Monitor conditions	
Detect and decide when problems exist that require service action	X
Protect the machine from damage when problems are detected	X
Isolate problems and determine the repair required	X
Alarm the operator and technician to problems and communicate control action needed	X
Provide automatic troubleshooting aids: display relevant values, provide diagnostic tests and calibrations	X
Detect and decide when problems are fixed	

Table 4: Service Responsibilities – Operator (OP)

General Responsibilities	Specific
Operate the equipment in a way that does not lead to machine damage	
Monitor equipment condition and alarms	
Maintain the equipment: Applicable to loss event listed below	
Check and maintain hydraulic oil level	X
Change oil filter (when restricted or per regular interval?)	
Respond to problems that occur	
Follow DTC and operator manual instructions	X
Request service support	
Communicate observed symptoms to service technician	

Table 5: Service Responsibilities - Service Technician (ST)

General Responsibilities	Specific
Find technical information related to problem	
Follow service instructions (includes using required special tools, torqueing hardware to correct specification, following diagnostic steps, etc…)	X
Perform diagnostic procedures and checks	X
Determine the repair required	X
Request escalated service support	X
Communicate observed symptoms and service actions taken	
Request parts needed for repair	
Repair the equipment	
Verify repair	
Document time and repair steps taken for payment and warranty	

Table 6: Service Responsibilities – Product Support (PS)

General Responsibilities	**Specific**
Resolve problems quickly to minimize customer downtime	X
Develop operating and service training content	X
Deliver training	
Develop technical information (service procedures, operating instructions, parts information)	X
Ensure technical information is easy to find, correct, and complete	X
Provide technical assistance through TAC	X
Provide technical assistance through field support staff	
Monitor design changes and update technical information	
Provide service parts	
Develop and provide service tools	
Provide input into new designs to enable learning from past experiences.	
Document problem reports and escalate issues to product design	X
Update technical information based on problem reports	

Table 7: Service Responsibilities – Management (MT)

General Responsibilities	**Specific**
Define and track metrics to drive decisions that optimize machine availability	X
Define and enforce serviceability controls within the design process	X
Define serviceability standards, design guidelines, and analysis techniques.	X

3.5 CAST Step 3: Analyze Each Component

3.5.1 Analyze the Physical Loss

This section analyzes the loss in terms of the physical system and controls. In general, physical diagnostic controls may consist of:

- Physical gauges used to provide feedback needed for diagnostics. Physical gauges are often required when an electrical sensor is not included in the design.
    - Examples: Oil level sight gauge or dipstick, tire tread wear gauge
- Diagnostic check points used to manually verify feedback needed for diagnostics.
    - Examples: Pressure ports and diagnostic receptacle (DR) fittings, electrical connectors used for pin out tests, visual inspection points
- Providing adequate access to the diagnostic check points and physical gauges.

Physical design requirements for hazard mitigation:

Specific to this loss event, the following physical service constraints were violated.

- SC-7: If the machine is unable to pin point the repair required, adequate diagnostic feedback check points must be provided. (H-2, H-4)

Physical controls included in the design to prevent this type of diagnostic loss:

Specific to this loss event, the following physical controls were included in the design.

- MG oil level gauge (dipstick)
- Diagnostic receptacles
    - One for each of the five PST clutches
    - Supply pressure, located on the MG
- Access to diagnostic receptacles
- Access to pressure sensors

What physical failures happened that led to the hazards?

One common physical failure occurred relevant to the diagnostic loss. Several cases confirmed a supply pressure sensor failure (PP.CHS-1). However, many of the sensors returned tested no-fault-found. The sensor failures, coupled with an inadequate ability to isolate sensing system problems, led to the replacement of many sensors and excessive diagnostic time. (*Question: Are sensor test conditions representative of operating environments? [Unknown]*).

What interactions happened that led to the hazards?

One unexpected system interaction was identified (PP.CHS-2). This unexpected interaction contributed to the hazard, because the machine falsely indicated a problem. The system detected low pressure on startup before the system stabilized. This was a normal operating condition, that didn't require any service action. However, the DTC logic did not account for the stabilization time, and falsely indicated a problem. The DTC mislead the operator to thinking service action was needed.

Missing or inadequate controls that may have prevented the loss:

The following physical diagnostics were either missing or inadequate. This section begins to highlight potential design changes to address the issue. All CAST generated recommendations are summarized in section 3.7.

- Missing oil level gauge on the sump (PP.CHS-3). There was no way to either automatically or manually check the oil level in the sump.
- Missing and inadequate diagnostic check points for measuring pressure between the valves and actuators (PP.CHS-4). This pressure was needed to isolate problems with the valve and the actuator. There were eleven actuators on the same pressure circuit. Of these eleven actuators, only one had a pressure sensor and only six had diagnostic receptacles (DR).
- Missing diagnostic check points to verify supply pump and scavenge pump flow and pressure (PP.CHS-5). Checking pump functions was a time consuming, messy task because it required disconnecting hydraulic hoses. Installing a flow meter required several special fittings, which the service technician may not have available. Checking pump pressure required disconnecting hoses, re-plumbing the circuit, and installing a DR. These controls were inadequate, because it took just as long to verify pump flow with a gauge as it took to replace the pump.

Table 8 summarizes the physical contributions to the hazardous state (CHS) discussed above. Each CHS is labeled so it can be traced to contextual factors and recommendations.

Table 8: Summary of Physical Contributions to the Hazardous State

CHS ID	CHS Description
PP.CHS-1	Sensor problems
PP.CHS-2	Unexpected system interaction
PP.CHS-3	Missing oil gauge

PP.CHS-4	Missing and inadequate actuator pressure diagnostic check points
PP.CHS-5	Missing pump diagnostic check points

Contextual Factors:

Next the analysis considers why the physical system contributed to the hazards. It explores answers to the following questions: Why did the physical failures and inadequate interactions occur and why did they contribute to the hazard? Why were controls missing or inadequate and why did they contribute to the hazard?

Contextual factors that explain why the contributions occurred are summarized in Table 9. For example, one contextual factor was the evolution of the system complexity over time (PP.F-6). Two gearcases and nine actuators were added to an existing hydraulic circuit while attempting to minimize design changes to legacy components. The previous system also had missing diagnostic controls, but it was less complex and easier to diagnose. While diagnostics were not optimized, they were acceptable. Based on this precedent, the legacy diagnostic designs were carried forward into the more complex system. This contributed to an unacceptable diagnostic time, because the system diagnosibility did not keep pace with the system complexity.

Table 9: Physical CHS Contextual Factors

ID	Contextual Factor
PP.F-1	The sump was designed to be empty during operation. Operators do not check or fill sump oil as part of scheduled maintenance activities. (PP.CHS-3)
PP.F-2	There were several other gear pump systems on the machine, none of which could detect pump malfunctions. The design precedent did not include pump diagnostic controls. (PP.CHS-5)
PP.F-3	Diagnostic check points add product cost. (PP.CHS-3, CHS-4, PP.CHS-5)
PP.F-4	Program metrics. (PP.CHS-3, CHS-4, PP.CHS-5)
PP.F-5	Space constraints. (PP.CHS-4)
PP.F-6	The system evolved over time, adding functions to the existing MG oil circuit. When nine actuators and two gearcases were added, diagnosing low supply pressure became more difficult. (PP.CHS-2, PP.CHS-4)
PP.F-7	Development process and guidelines. (PP.CHS-3, CHS-4, PP.CHS-5)
PP.F-8	Service technicians and TAC specialists often assumed sensor problems due to historical issues. (PP.CHS-1)

3.5.2 Analyze Each Component

This section moves up the control structure to understand each element's contribution to the hazard and explore why each controller did what it did. Each controller's actions, inactions, and decisions are considered and explained. While examining "why", it was assumed that the humans in the system wanted to do the correct thing and did what they thought was best at the time. This assumption is key to avoiding blame and hindsight bias in the analysis. Contextual factors, such as the increasing system complexity over time, identify weaknesses in the control structure and remove blame from the analysis.

To explain "why", the analysis considers contextual factors and flaws in the process models at the time of the loss event. For example, these might include incorrect or insufficient information available at the time, inadequate training, other pressures or incentives, and misleading feedback. The examination of each component includes several parts as described in Leveson's CAST Handbook (Leveson, 2019):

- Component responsibilities related to the loss event
- Contribution (actions, lack of actions, and decisions leading to the hazardous state)
- Why? Flaws in the mental/process model contributing to the actions
- Why? Contextual factors explaining the actions, decisions, and process model flaws

For example, one mental model flaw that contributed to many functioning sensors being replaced was the assumption of sensor failure by the service technician (PP.F-8). Historical sensor problems contributed to people believing that replacing the sensors was the most likely repair needed to resolve the DTC. Instead of completing a thorough troubleshooting procedure to confirm a sensor problem before replacing it, the service technician just replaced the sensor. Time pressures also contributed to the replacement of good sensors. Replacing the sensor takes less time than following the troubleshooting procedure. When a machine is down, service technicians will do whatever they believe is fastest to resolve the problem.

Traceability is maintained throughout the component analysis. Many of the contextual factors affected multiple system elements and their contributions to the hazardous state. References to previously identified contextual factors are included in each of the applicable system elements for traceability. Trying to explain "why" also raised many questions. These questions are included and traced to answers found. Unanswered questions are identified for potential use in further analysis of the out of scope elements such as the dealer/service shop.

This section contains analysis details for a few of the key system elements, analyses of the remaining system elements can be found in the CAST Details Appendix.

Physical Process Control System (Machine PCU)

Service-Related Responsibilities

- PCU.R-1: Detect and decide when problems exist that require service action (SC-1, SC-2)
- PCU.R-2: Protect the machine from damage when problems are detected
- PCU.R-3: Isolate problems and determine the repair required (SC-5)
- PCU.R-4: Alarm the operator and technician to problems and communicate control action needed (SC-3, SC-4, SC-8)
- PCU.R-5: Provide automatic troubleshooting aids: display relevant values, provide diagnostic tests and calibrations (SC-7)

Control Actions Contributing to the Hazard

- PCU.CHS-1: The process control system did not adequately determine when low supply pressure required operator or technician action. False positive DTCs were triggered on start up when supply pressure was low due to normal operating conditions that did not require service action. (PCU.R-1, PCU.R-4)
- PCU.CHS-2: The process control system prevents machine movement when low supply pressure is detected on startup. This forces unplanned downtime when the DTC is active. It may also limit the system's ability to isolate problems with the transmission. (*Question: Can the clutches be tested for slip, indicating actual low pressure? [Unknown]. If so, this could be added as a diagnostic test.*)
- PCU.CHS-3: The process control system did not adequately isolate problems or determine the repair required. This left a large number of potential repairs (like replace valve, repair harness, replace sensor, replace pump, etc…) for the service technician to troubleshoot and decide between. (PCU.R-3)
- PCU.CHS-4: The process control system over-alarmed the operator by sometimes triggering multiple alarms. (PCU.R-3, PCU.R-4)
- PCU.CHS-5: The process control system did not issue the operator control action desired. The DTC contained no information about what the operator was supposed to do. When operator action is not clearly communicated, operators will typically ignore the alarm or call for service support instead of taking the desired operator action. (PCU.R-4)
- PCU.CHS-6: The process control system did not provide interactive diagnostic tests to enable isolating problems between the AST, PST, and MG. (PCU.R-5)

Why? Process/Mental Model Flaws

- PCU.F-1: Inadequate DTC logic. Missing requirements to consider environmental conditions. Incorrect assumptions hydraulic system interactions. Thresholds used on legacy design no longer applied due to system evolution. (PCU.CHS-1)
- PCU.F-2: Process model flaw that when low pressure feedback is received, the system pressure is actually low. (PCU.CHS-3). (*Question: Why were DTC software requirements missed? [*PP.F-7]*)*
- PCU.F-3: Inadequate software logic to avoid situation X. *(Question: Why? [PCU.F-6]).* Missed software requirements and assumptions. (PCU.CHS-4)
- PCU.F-4: Missing information to isolate problems due to inadequate sensors provided. (PCU.CHS-3) (*Question: Why were inadequate sensors provided? [*PP.F-4, PP.F-7]*)*
- PCU.F-5: Missing DTC software requirements to monitor other system feedback to help isolate the problem. (PCU.CHS-3, PCU.CHS-4)

Why? Contextual Factors

The following contextual factors already identified apply:

- PP.F-4: Program metrics. (PCU.CHS-3, PCU.CHS-6)
- PP.F-7: Development process and guidelines. (PCU.CHS-1, PCU.CHS-3, PCU.CHS-4, PCU.CHS-51, PCU.CHS-6)

Additional contextual factors include:

- PCU.F-6: The process control system's responsibility to protect system from damage potentially conflicted with the responsibility to determine the repair required. In this situation, software design requirements prioritized protecting the system from damage. (*Question: Why? What criteria is involved in this design decision? [PP.F-7]*) (PCU.CHS-2)
- PCU.F-7: Individual DTC software logic becomes complex to avoid situation X. (PCU.CHS-4*)*

Service Technician (ST)

Service-Related Responsibilities

- ST.R-1: Follow service instructions
- ST.R-2: Perform diagnostic procedures and checks
- ST.R-3: Determine the repair required
- ST.R-4: Request escalated service support

Control Actions Contributing to the Hazard

- ST.CHS-1: Service technician didn't start by checking the oil level or checked the wrong oil level. (ST.R-1)
- ST.CHS-2: Service technician didn't complete diagnostic instructions before replacing sensors or other parts. (ST.R-1, ST.R-2)
- ST.CHS-3: Service technician decided on the wrong repair and replaced good parts. (ST.R-3)
- ST.CHS-4: Service technician requested TAC service support before completing diagnostic procedures. (ST.R-4)

Why? Process/Mental Model Flaws

- ST.F-1: Service technician didn't know low oil level could cause the low pressure DTC. DTC did not communicate to check oil level. DTC instructions in the technical manual (TM) did not include instructions to check the oil level. (ST.CHS-1) (*Question: Why did the diagnostic procedure not cover checking oil level? [PS.CHS-1])*
- ST.F-2: Checked the wrong oil level and thought oil level was OK. Did not know there were two hydraulic reservoirs on the machine or did not know which hydraulic circuits pulled from which oil reservoir. (ST.CHS-1)
- ST.F-3: Service technician believed the replacing the sensor was the most likely repair required. Instead of completing a thorough troubleshooting procedure to confirm a sensor problem before replacing it, the service technician started by replacing the sensor. *Why?* Step one in the TM is to swap the AST pressure sensors and check the diagnostic addresses. This may create a bias towards sensor issues. (ST.CHS-2, ST.CHS-3). History of sensor problems set a precedence of replacing sensors as a first troubleshooting step. (PP.F-8)

Why? Contextual Factors

The following contextual factors already identified apply:

- PP.F-8: History of sensor problems created bias to assuming sensor problem (PCU.CHS-2)

Additional contextual factors include:

- ST.F-4: Harvest is a critical and rushed time of year. When machine problems happen, customers are dissatisfied and need the equipment up and running as fast as possible. Unplanned service is a high pressure situation. Service technicians do whatever they think will fix the problem quickly. (ST.CHS-2, ST.CHS-3, ST.CHS-4)
    - PP.F-9: Sensor is quicker to replace than troubleshooting it
    - Diagnosing the hydraulic system requires disconnecting hoses and having a lot of different sized fittings to manually check pressure and flow. Manually checking pump flow can take as much time as replacing a hydraulic pump. Related to PP.CHS-5: Missing pump diagnostic check points
    - Learning theory of operation on the spot is time consuming due to complexity of equipment. (*Question: Is training adequate? [Unknown, see PS.CHS-6])*
- ST.F-5: Service technicians support all types of agricultural equipment. The service technician responding to the problem may not be an expert on this system. (ST.CHS-1, ST.CHS-3, ST.CHS-4) *(Question: Does training enable general knowledge and expert, system specific knowledge? [Unknown, see PS.CHS-6])*
- ST.F-6: The machine may be stuck in the field without access to typical service tools and equipment available in a shop. (ST.CHS-2, ST.CHS-4)
- ST.F-7: Diagnostic procedures are complicated. (ST.CHS-2, ST.CHS-4) (*Question: Why are diagnostic procedures complicated? [PS.CHS-3])*
- ST.F-9: Technical information differs between the sources of information. (ST.CHS-2, ST.CHS-4) *(Question: Why? [Unknown])*
- ST.F-10: The diagnostic procedure doesn't call out using the supply pressure DR. (PP.CHS-1)
- ST.F-11: Culture of replacing electrical control units and updating software to resolve problems. System diagnostics takes longer than replacing components. (ST.CHS-3)
- ST.F-12: System complexity rapidly increased, reducing human ability to understand how the system works. (ST.CHS-2, ST.CHS-3, ST.CHS-4)
- ST.F-13: The skill level of technicians widely varies. Technician may not have had adequate experience, training, or work instructions. Due to industry service technician shortage, it can be difficult to find qualified service technicians to hire. (ST.CHS-2, ST.CHS-3, ST.CHS-4) *(Questions: What work instructions were provided for this system or DTC? [Unknown] What real-time technical assistance did the service shop/dealer provided to the service technician? [Unknown] Were system experts available as resources for the service technician? [Unknown] If not, why?)*

Product Support (PS)

Service-Related Responsibilities

- PS.R-1: Resolve problems quickly to minimize customer downtime (SC-6, SC-10)
- PS.R-2: Develop service training content
- PS.R-3: Develop service instructions & diagnostic procedures (SC-6)
- PS.R-4: Ensure technical information is easy to find, correct, and complete (SC-3, SC-8)
- PS.R-5: Provide technical assistance through TAC (SC-10)
- PS.R-6: Document problem reports and escalate issues to product design (SC-10)

Control Actions Contributing to the Hazard

- PS.CHS-1: DTC diagnostic instructions did not include checking MG oil level. (PS.R-4)
- PS.CHS-2: Step one in the TM is to swap the pressure sensors and check the diagnostic addresses. This may create a bias towards sensor issues. (PS.R-3, PS.R-4)
- PS.CHS-3: Diagnostic procedures are complicated. (PS.R-4)
- PS.CHS-4: TAC sometimes suggested replacing parts before completing troubleshooting procedure. (PS.R-1, PS.R-5)
- PS.CHS-5: Inadequate feedback to product design. (PS.R-6)
- PS.CHS-6: *Questions: What information specific to this system is included in training content? Are general theory of operation and diagnostic methods for hydro-electric systems adequate? Is service training content adequate for the level of equipment complexity? Is service training content up to date and correct? Are service technicians incentivized to take training? Are technicians re-trained at an adequate frequency? [Unknown]*

Why? Process/Mental Model Flaws

- PS.F-1: Product support specialists expect a certain level of operator and service technician knowledge. (PS.CHS-1, OP.CHS-1)
- PS.F-2: Product support specialists assumed DTC is most likely to be a problem with component X. (PS.CHS-2, PS.CHS-3)

Why? Contextual Factors

The following contextual factors already identified apply:

- PP.F-4: Program metrics. (PS.CHS-3, PS.CHS-5)
- PP.F-7: Development process and guidelines. (PS.CHS-3, PS.CHS-5)
- PP.F-8: History of sensor problems created bias to assuming sensor problem. Swapping existing sensors first is a quick and easy way to confirm if it's a sensor problem before recommending installing a new sensor. (PS.CHS-2, PS.CHS-4)

- SS.F-2: Conflicting responsibility to resolve problems quickly and ensure adequate diagnostics before replacing parts. (PS.CHS-4)
- ST.F-12: System complexity rapidly increased, reducing human ability to understand how the system works. (PS.CHS-3, PS.CHS-4)
- PD.F-5: System complexity increased over time reducing diagnosibility.

Additional contextual factors include:

- PS.F-3: System complexity increased the time and effort required to develop diagnostic instructions and diagnostic training. This also increased the complexity of the diagnostic instructions, inherently making them more difficult to follow. (PS.CHS-3, PS.CHS-4) *(Question: Was the increased effort required adequately captured in product support resource calculations? [Unknown])*
- PS.F-4: Electrical and software content rapidly increased over time, affecting the ability of humans to understand how the system works. (PS.CHS-6). (*Question: Has training content sufficiently kept up to adequately train service technicians? Has training kept up to adequately training TAC specialists and technical authors? Has technical information delivery methods kept up? [Unknown])*
- PS.F-5: Time pressures and technical authoring resource constraints. (PS.CHS-1, PS.CHS-3).
- PS.F-6: TAC specialists diagnose the problems remotely. Without access to the equipment, they rely on the service technician for information. Feedback and information needed to provide correct service instructions was often missing or inadequate. Miscommunications between TAC specialist and service technician occurred. (PS.CHS-4)
- PS.F-7: Inadequate feedback on service control effectiveness. (PS.CHS-3, PD.CHS-2)

3.6 CAST Step 4: Identify Control Structure Flaws

This section takes a step back from the individual system elements to consider the system as a whole. The purpose is to identify systemic factors that negatively affect the whole system or multiple system elements. Common examples include communication and coordination, information systems, culture, changes in the system over time, and economic factors. Considering these systemic factors provides another way to understand why individual components did not fulfill their responsibilities.

The first two systemic factors discussed below were identified in the previous component analysis. The discussion below further explores these systemic factors and summarizes their effects on the whole system.

ST.F-12: Rapid technology change and increased complexity

Technology changed rapidly and the electrical and software content on agricultural equipment increased very quickly. This rapid change affected all parts of the sociotechnical system. Agriculture equipment manufacturers were traditionally "big-iron" companies. Service shops and dealerships traditionally focused on mechanical repairs. Their processes and knowledge management systems were created when equipment was primarily mechanical. As technology rapidly changed and product complexity quickly increased, meeting customer service needs required new processes, updated training, and new employee skillsets. The established processes struggled to keep pace with rapidly changing customer and service technician needs, contributing to the diagnostic loss event. It may have also affected the service shop's ability to adequately train and staff technicians with the required skillsets.

The fast pace of change also affected how well the design engineers, product support personnel, operators, and service technicians understood the system behavior. For example, designing DTC software required an expert understanding of the entire system and the system interactions. Inadequate system based techniques led to missed interactions between systems and DTCs.

As another example, the operators and service technicians struggled to understand the new system due to the large number of interfaces. Even the basic task of checking oil level was complicated by the system complexity. Known cases of people checking the wrong oil level indicated an inadequate understanding of the system. More intuitive designs, more effective training, and more efficient service instructions were needed to support operators and technicians working with the complex system.

ST.F-4: Time-pressured environment

Another systemic factor was the external time pressures associated with a harvest operation. Due to weather and environmental factors, harvest is a high-pressure, limited time of year. There is often a narrow window of time to harvest crop with optimized yields. Any machine unavailability can

significantly affect farm operation financials. The cost of downtime is extreme, therefore all parties responsible for machine service typically prioritize fixing problems as fast as possible.

This system factor affected the actions of TAC specialists, service technicians, and operators. In this loss event, the machine couldn't pinpoint the repair required. This left it up to the service personnel to troubleshoot and figure out the correct repair. Many of the diagnostic checks took longer than replacing parts, which contributed to swapnostics. The order in which the service technicians replaced parts or in which the TAC specialists recommended part replacements, highly depended on their mental model of the most likely repair needed. The rushed environment contributed to the decisions to swap parts before completing troubleshooting procedures. The service technicians and TAC specialists were doing the best they could to fix the problem quickly and get the machine back up and running.

The time pressures affected post-production operations, but it also affected pre-production field testing. Harvest is a limited time of year, and field testing was rushed to complete required tests. Field testing had to ensure machines accumulated sufficient duty cycle hours to verify machine durability. Any machine unavailability posed a risk to successfully verifying the equipment. Due to these time pressures, field test personnel prioritized fixing problems quickly over validating product serviceability. It was faster to leverage their personal system knowledge or call an engineer that designed the system for quick troubleshooting help, then to follow the troubleshooting procedures in the technical manual.

Reliability Focused Culture

The reliability focused development culture also systemically affected the service control structure. Customers cared about reliability, because it affects machine availability. However, they also cared about serviceability as another key contributor to machine availability. Product development followed the reliability culture and focused on designing out problems. Serviceability was underutilized as a control to minimize the customer loss when problems do occur.

Diagnostic and repair time increased gradually in the ten years prior to this loss event. The longer diagnostic and repair times contributed to more machine downtime, eventually increasing it to an unacceptable level. Historically, machines were easier to service and understand. Prior to the industry labor shortages, service shops might have attracted more service technician applicants with the required skillset. In this previous context, reliability may have been the most important product element of machine availability. The manufacturer may not have adequately reacted to these gradual changes in the ecosystem. As equipment serviceability degraded over time, the reliability focused view of machine availability did not capture the holistic customer need.

The reliability culture was apparent throughout the service control structure, including management, product design, product test, and product support. It contributed to machine availability metrics that mainly focused on reliability. It also contributed development processes focused on designing out failures as a way to deliver machine availability. Product design and testing mainly focused on improving reliability as the way to deliver machine availability. Product support focused on providing feedback to the design teams to improve reliability. The reliability focused culture unintentionally contributed to the diagnostic loss event.

Communication and Coordination

Communication and coordination were other important systemic factors. Communication through the service escalation chain was similar to the childhood game of telephone. One person started a message and passed it on to another. That next person told another person, and so on. By the end, after passing the message multiple times, it was rarely the same message from beginning to end. Starting from when an operator called for support to when the problem was resolved, important information about observed symptoms and actions taken was misconstrued. As support escalated, the people involved in helping diagnose the problem were further removed from the operator and the equipment, physically and in the communication chain. This may have contributed to missing information about observable symptoms, misinformation about what was checked already, and other communication mishaps.

Another aspect of communication that affected the manufacturer was communication between the teams involved with the system pre-production and the teams involved with the system post-production. The product development engineers worked on the system until it went to production, and then they shifted to the next project. This handoff to a continuous improvement engineering team required communication and coordination. Another communication handoff was between product design and product support. Product support needed information about the system, including schematics, DTC software requirements, models, and design rationale information to create training content and service instructions. It is unknown how adequate these handoffs were, but they may have contributed to the varying post-production product support effectiveness. Inadequate communication between groups may have also affected the ability of product development to learn from past issues.

After analyzing each element and the control structure as a whole, Figure 19 summarizes the key controls and feedbacks that were missing or inadequate in this diagnostic loss event. Recommendations in the next section focus on strengthening the control structure elements shown in red. The dealer/service shop and the farm operation were out of scope for this analysis. While their controls on the operator and service technician may have been inadequate, they are not highlighted red in the figure below.

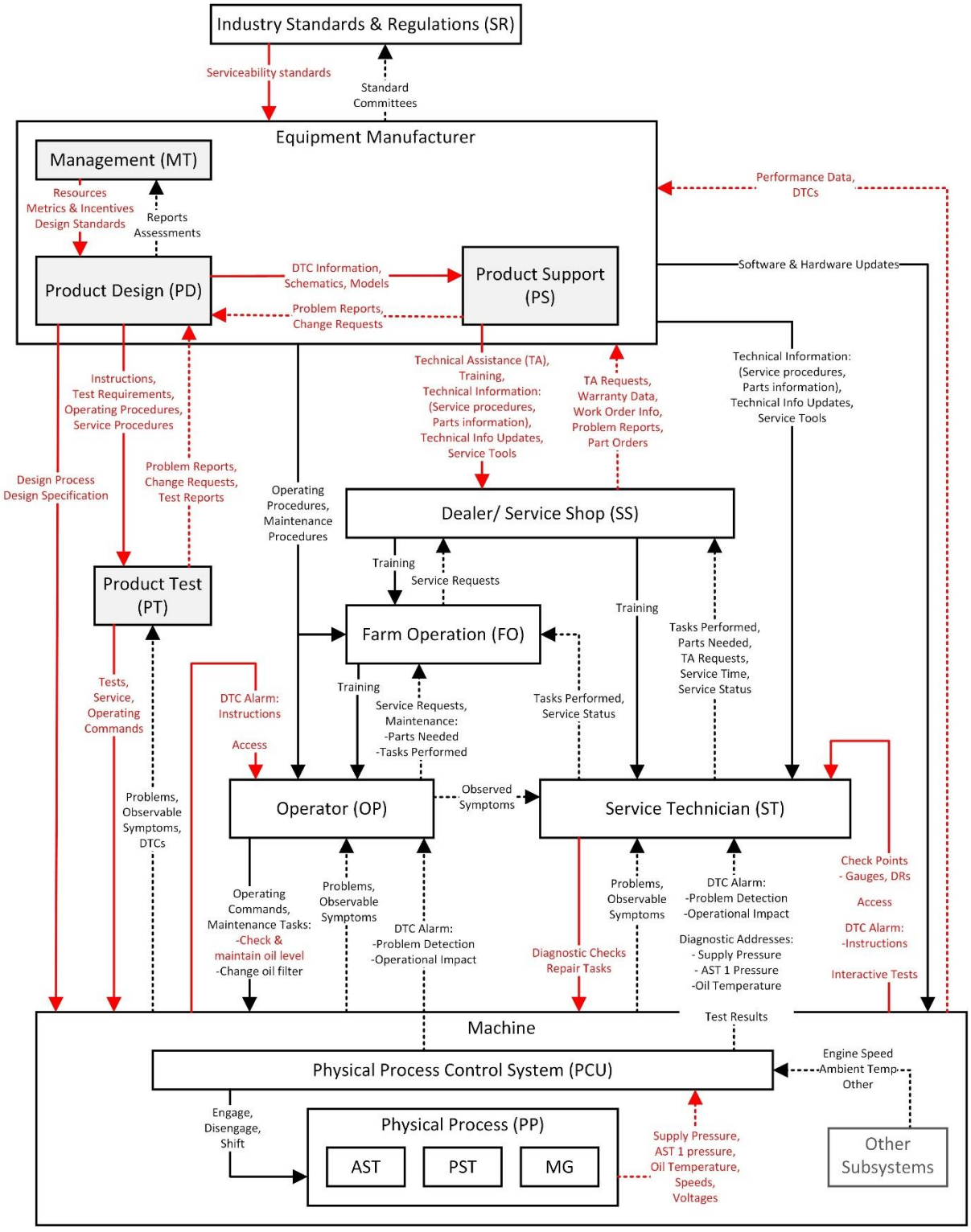

Figure 19: Missing or Inadequate Controls and Feedback

3.7 CAST Step 5: Create Improvement Program

This section discusses potential physical process and control structure improvements that address the diagnostic loss and prevent future losses. It also summarizes questions generated that could be used to further investigate other elements in the system, such as the farm operation and the dealer/service shop. The author recognizes that these recommendations come with tradeoffs not considered in this analysis, so no attempt was made to prioritize the recommendations. It is the author's hope that the results can be used to make design and process changes to improve future product serviceability.

Recommendations for the Physical Process:

- Add an oil level gauge or sight plug (PP.CHS-3)
- Add diagnostic receptacles (DRs) (PP.CHS-4)
- Improve pump flow and pressure verification methods to reduce time to diagnose pump problems. (PP.CHS-5)

Recommendations for the Physical Process Control System:

- Add self-diagnostic capabilities to better isolate or narrow down the repair required. (PCU.CHS-3)
- Update the DTC to include instructions to check oil level and drive the desired operator behavior. (PCU.CHS-5)
- Conduct a system DTC analysis. (PCU.CHS-4).
- Update DTC logic to consider other system conditions that could help isolate the repair required. (PCU.F-5)
- Add an interactive diagnostic test that isolates clutch engagement problems. (PCU.CHS-6)
- Increase remote access capabilities to machine information needed for diagnostics. (PS.F-6)

Recommendations for Product Support:

- Update diagnostic instructions to:
    - Add checking MG oil level (ST.F-1)
    - Use supply pressure DR to verify pressure instead of removing the pressure sensor and installing a DR (ST.F-10)
    - Consider ways improve readability (PS.CHS-3)
- Revise TAC solutions (ST.F-9)
- Strengthen feedback structure to monitor effectiveness diagnostic controls and drive improvements based on feedback. (PS.F-7)

- Implement feedback system to monitor effectiveness of DTCs post-production and drive DTC design improvements based on feedback. (PS.F-7)
- Implement a single source of technical information. (ST.F-9)
- Communicate diagnostic pain points and lessons learned to product design and engage in diagnostic reviews to provide expert input. (PS.CHS-5)
- Investigate diagnostic training effectiveness for service technicians. (ST.F-5)
  Questions to answer:
  - *Is training content and delivery adequate for general diagnostic techniques, electrical and hydraulic systems, and this specific system?*
  - *Are dealers incentivized to train or certify service technicians?*
  - *Has training content sufficiently kept up with new technologies and the level of system complexity?*
  - *Are technicians re-trained at an adequate frequency?*

Recommendations for Product Design:

- Leverage systems theory STPA technique to manage system complexity and develop system diagnostic requirements. (PD.F-4)
- Involve product support in diagnostic discussions to incorporate lessons learned from past designs. (PD.CHS-3)
- Conduct diagnostic reviews to identify opportunities to improve self-diagnostic capabilities. (PD.CHS-1)
- Ensure DTCs clearly communicate the operator or service technician action required and drive the desired behaviors. (PD.CHS-2)
- Document DTC design information and diagnostic design review information for downstream users, such as product support personnel. (PD.CHS-4)
- Avoid reliability-focused view of machine availability. Consider serviceability and reliability simultaneously to optimize machine availability. (PD.F-12)
- Consider a different DTC architecture that reduces DTC logic complexity. (PCU.F-7)

Recommendations for Product Test:

- Report nuisance and ineffective DTCs during field and lab testing. (PT.CHS-1)
- Report DTC experienced during field or lab testing. (PT.CHS-1)
- Report when a problem takes longer than X hours to diagnose during field or lab testing. (PT.CHS-1)

- Leverage diagnostic procedures to diagnose problems to help verify the procedures. (PS.F-5)
- Document what data is used to diagnose a problem and communicate to product design. This could help identify missing feedback for DTC logic and missing diagnostic addresses. (PT.F-9)

Recommendations for Management:

- Develop metrics and incentives that optimize machine availability by simultaneously considering reliability and serviceability. (MT.CHS-1)
- Strengthen project metrics. (PP.F-4)
- Develop diagnostic design guidelines, standards, and best practices. Ensure tools and processes enable following the guidelines. (MT.CHS-2)
- Develop design guidelines and decision criteria evaluate the customer uptime impact of a protection shutdown. (PCU.CHS-2)
- Define responsibilities for DTC verification and enforce the roles and responsibilities. (PT.F-2)
- Ensure DTC software is complete before field testing to enable verification of DTCs. (PT.F-4)
- Define responsibilities for emergent properties and system interfaces that span design team responsibilities. (PD.F-4)
- Define responsibilities for serviceability verification and enforce the roles and responsibilities. (PT.F-2)
- Define serviceability goals. Enable and incentivize product development teams to produce designs that meet the goals. (PD.F-11)
- Develop better controls for verifying diagnostic procedures are completed and effective prior to production. (PS.F-5)

This case study demonstrated that CAST methodology effectively examines serviceability issues. The analysis identified over thirty-five recommendations for both the physical process and development processes. These recommendations, if applied, will improve the serviceability of this system and help prevent similar issues on future systems. Questions were also generated that could be used for further investigation into the service shop/dealer contributions and into the farm operation contributions. Insights about applying CAST to serviceability are summarized in section 5.1.

4 Case Study 2: Serviceability STPA of Future System

The purpose of this case study is to explore how STAMP based tools can be used for serviceability by analyzing a future system using STPA. This section reveals that STPA can be extended to serviceability, and that a service STPA successfully generates serviceability constraints and recommendations in an early conceptual design phase.

The analyzed system, the "TI system", incorporates automation into an existing machine function. The system includes an electrical control unit, sensors, physical process control software, operator interface software, and DTC service alarm software. Key interfaces includes the TI operator interface and TI interfaces with existing machine systems.

At the time of this analysis, the system was in an early conceptual phase, with few known design details. The system was specifically chosen to demonstrate that STPA is an effective "design for" method. It was also chosen because it's a software-intensive system with important operator interfaces. STPA is not limited to physical components, and this case study demonstrates STPA's ability to generate software and operator interface requirements.

The case study also begins to explore if elements of a safety STPA are applicable to a service analysis. After completing a partial safety analysis, a full STPA was conducted focusing on serviceability. The purpose of starting with the safety review was to understand if any of the analysis elements could be shared or reused between safety and serviceability. Insights about similarities between the safety analysis and service analysis are captured in the recommendations and conclusions section, but the safety analysis details are not included.

The following sections step through the service analysis and capture the generated service requirements. Assumptions are documented throughout the process. As the system is further developed and design decisions made, these assumptions can be revisited to ensure the design meets serviceability needs. The system and analysis details cannot be disclosed due to the proprietary nature of the project, so details are generalized and removed where necessary.

4.1 STPA Step 1: Define the Purpose of the Analysis

The goal of the analysis is to identify serviceability constraints for a future system design. The losses defined are serviceability losses, and the hazards capture various aspects of serviceability. The boundary for the analysis is shown in Figure 20. The service technician and operator are considered inside the boundary of the analysis because system design must include controls that drive the desired operator and service technician behavior for maintaining, repairing, and diagnosing the machine. Also inside the boundary of the analysis is the technical information that specifies service instructions. Other machine systems are outside the analysis boundary. Product development processes, product support processes, and other elements like the service shop are also outside the scope of the analysis.

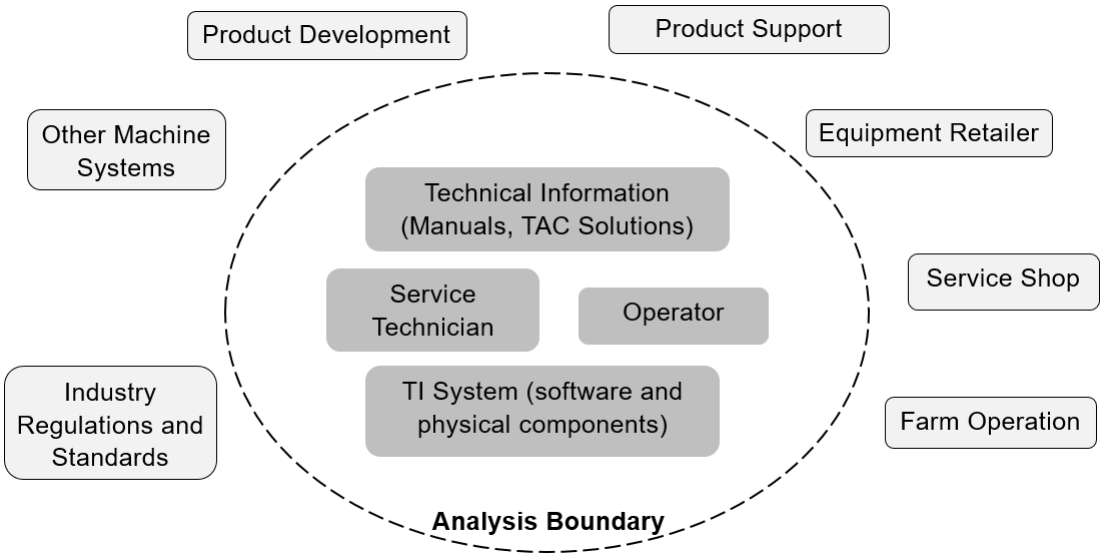

Figure 20: Service STPA Boundary

Three important losses are considered in this analysis. These are the same losses that occurred in the diagnostic loss event analyzed in the CAST case study. These losses may often apply to service STAMP-based analysis.

- Unplanned downtime due to inadequate serviceability (L-1)
- Financial losses incurred through warranty costs (L-2)
- Customer dissatisfied (L-3)

Several different hazards can lead to these losses. Table 10 summarizes the high level system hazards and system service constraints. The system constraints must be enforced to prevent the hazards. System constraints may also exist to minimize the losses if the hazard occurs. For example, to prevent the technician from doing the wrong repair the machine must identify the correct repair. However, if the machine is unable to pinpoint the repair, the diagnostic troubleshooting procedures must lead the technician to the correct repair. This minimizes the unplanned downtime associated with the loss event. Each hazard is traced to the applicable losses and each system constraint is traced to the applicable hazards.

Table 10: Service STPA Hazards and System Constraints

Hazard ID	Hazard	ID	System Service Constraint
H-1	Operator takes the wrong action to mitigate the problem (L-1, L-3)	SC-1	Machine must detect problems (H-1, H-2)
		SC-2	Machine must decide the operator action required (H-1)
		SC-3	Operating instructions must clearly communicate desired operator action (H-1)
H-2	Service technician does the wrong repair (L-1, L-2, L-3)	SC-4	Machine must pin point the correct repair required (H-2, H-4)
		SC-5	If machine is unable to pin point the repair required, troubleshooting procedures must identify the correct repair required (H-2, H-4)
		SC-6	Adequate diagnostic check points must be provided (H-2, H-4)
		SC-7	Service instructions must clearly communicate desired service technician actions (H-2, H-4)
H-3	Operator ignores a service alarm (L-1, L-3)	SC-8	Machine must prevent operator alarm fatigue (H-1, H-7, H-3)
H-4	Repair & troubleshooting time exceeds <X> minutes (L-1, L-2, L-3)	SC-9	Repair & troubleshooting time must not exceed <X> minutes (H-4)
		SC-10	Adequate access to perform diagnostic and repair tasks must be provided (H-2, H-4)
H-5	Service task (maintenance, repair, or diagnostics) introduces subsequent problems (L-1, L-2, L-3)	SC-11	Service tasks must not disturb unrelated systems or introduce subsequent problems (H-5, H-4)
H-6	Scheduled maintenance time exceeds <X> minutes over first <X> hours of use (L-3)	SC-12	Scheduled maintenance time must not exceed <X> minutes over first <X> hours of use (H-6, H-4)
		SC-13	Adequate access to perform maintenance must be provided (H-1, H-6)

4.2 STPA Step 2: Model the Control Structure

The hierarchical service control structure is shown below in Figure 21.

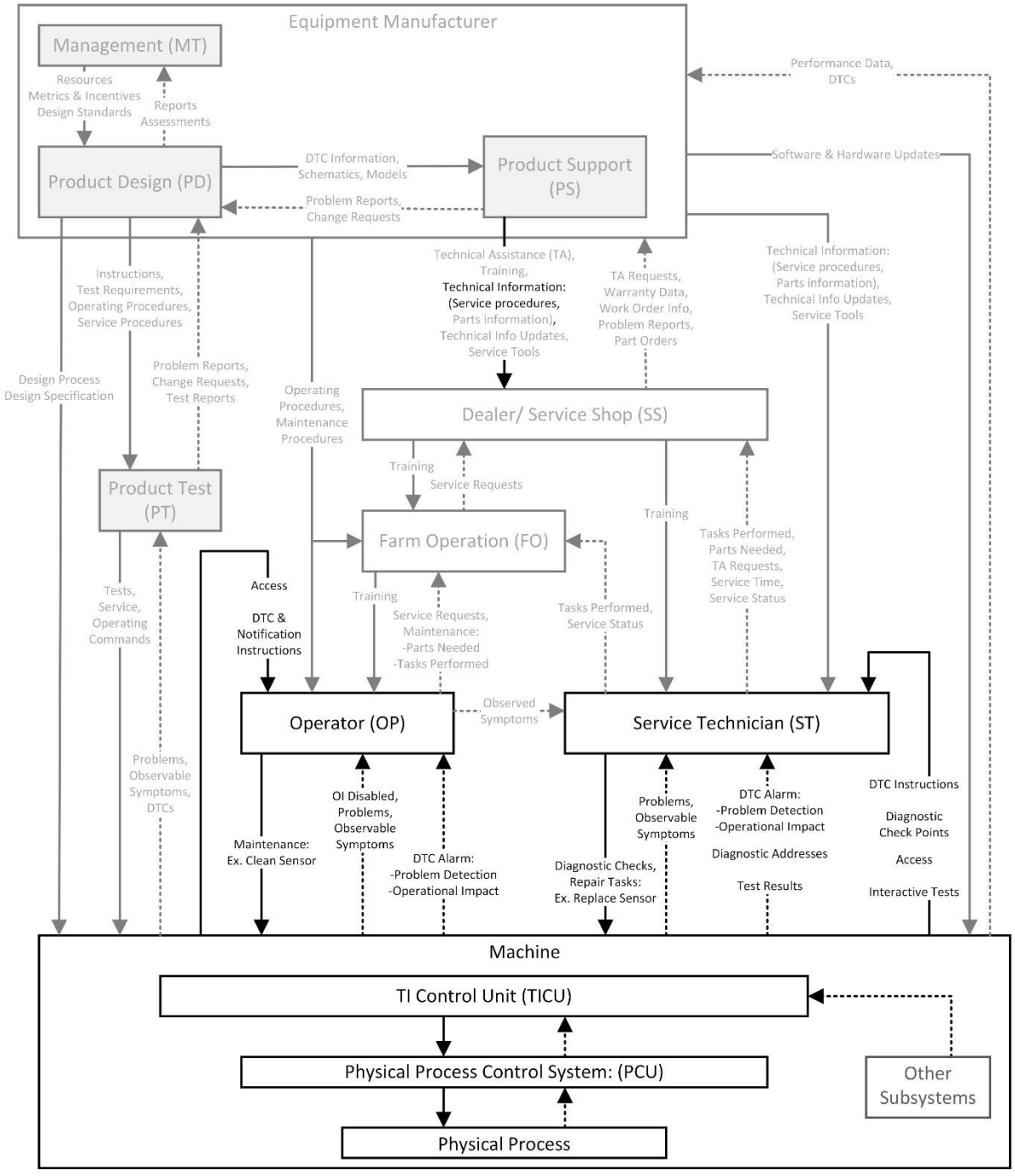

Figure 21: Service STPA Control Structure

Above the machine level, the control structure is the same structure used in the previous CAST analysis. The system elements and controls in black are the focus of this analysis. Other elements of the larger control structure are out of scope and greyed out in Figure 21. They were left in the figure to provide context for the analyst.

As described in section 3.4, CAST Step 2: Model the Control Structure, a key concept of the serviceability control structure is differentiating the role of the operator and the service technician. Whether or not they are the same person or employed by the same business isn't important for the hazard analysis. It is important to capture the different responsibilities between the operator and service technician. The operator is responsible for operating the equipment and maintaining the equipment. Preventative maintenance tasks, like cleaning windows or changing oil, are required on a regular basis to keep the equipment running. The service technician is responsible for diagnosing and repairing the equipment after problems occur. Wherever the machine does not self-diagnose problems, the service technician is responsible to troubleshoot and determine the repair required. They are also responsible for completing the repair and verifying the problem is resolved.

The previous CAST analysis also identified system element responsibilities. These general responsibilities are not repeated here. However, the specific service responsibilities of the physical process control system, operator, and technician are defined for the TI system. This step was very helpful for the analyst. It identifies the feedback required for the controllers to fulfill their responsibilities. Especially helpful is the holistic view of the feedback an operator needs to make correct control action decisions. At this point, requirements can be generated to capture feedback that must exist. This step produces requirement rationale by linking feedbacks to the responsibilities, aiding future design decisions.

Table 11: Service Responsibilities - Physical Process Control System (TICU)

ID	Responsibilities	Feedback Needed
TICU.R.1	Protect the system from damage when problems are detected (SC-1, SC-2)	
TICU.R.1.1	Automatically disable TI when problems are detected that will violate functional requirements	TI system health, Other system health
TICU.R.2	Determine the following operator actions required and provide operator instructions: (SC-1, SC-2, SC-3, SC-8, SC-12)	

TICU.R.2.1	Manually control the function because TI is disabled	TI disabled status
TICU.R.2.2	Clean TI sensors	Dirty sensor status
TICU.R.2.3	Adjust TI sensors	Sensor adjustment status
TICU.R.2.4	Perform TI calibration	Calibration status, Sensors out of range status
TICU.R.2.5	Check sensor to harness connection	Circuit voltages and currents
TICU.R.3	Decide if the following diagnostic or repair actions are required and provide technician instructions: (SC-4, SC-9)	
TICU.R.3.1	Differentiate between TI system problems and other system problems	Other system DTCs, PCU command X, TICU command X, machine operating conditions, circuit voltages and currents, communication signals
TICU.R.3.2	Differentiate between TI system problems and other sub-system problems (for example, if sensor power is lost, differentiate a sensor harness issue vs an electrical power generation problem)	Other sub-system DTCs, electrical system power, circuit voltages and currents, communication signals
TICU.R.3.4	Replace TI sensors	Sensor fault status, TI disabled/on/off status, DTC occurrence count
TICU.R.3.5	Replace TI controller	Circuit voltages and currents, communication signals, electrical system power
TICU.R.3.6	Troubleshoot and repair TI harnesses and connectors	Circuit voltages and currents, communication signals
TICU.R.3.7	Troubleshoot and repair sensor mounting	Sensor out of range, sensor adjustment status

Table 12: Service Responsibilities - Operator (OP)

ID	Responsibilities	Feedback Needed
OP.R.1	Operate the equipment in a way that does not lead to machine damage or machine unavailability	TI DTC alarms, other system DTC alarms, TI disabled status, machine operating conditions, visual monitoring
OP.R.1.1	Manually control the function because TI is disabled	TI disabled status (if not observable without an indicator, machine must provide active feedback), visual monitoring
OP.R.2	Maintain the equipment	Maintenance required indicator
OP.R.2.1	Clean TI sensors	Sensor dirty status (if not observable from the operator seat), visual inspection
OP.R.2.2	Adjust TI sensor position	Sensor adjustment status (if not observable from the operator seat), visual inspection
OP.R.2.3	Perform TI calibration	Calibration status
OP.R.2.4	Check sensor to harness connection	"check harness connection" DTC alarm, visual inspection

Table 13: Service Responsibilities – Service Technician (ST)

ID	Responsibilities	Feedback Needed
ST.R.6	Diagnose and repair the equipment	Repair required status
ST.R.6.1	Replace TI sensors	“replace sensor” DTC
ST.R.6.2	Replace TI controller	“replace controller” DTC
ST.R.6.3	Repair/replace TI harnesses and connectors	“troubleshoot and repair harness” DTC
ST.R.6.4	Repair/replace sensor mounting bracket	Visual access to sensor and mount
ST.R.6.5	Update TI software	Software update required status

4.3 STPA Step 3: Identify Unserviceable Control Actions (UCA)

This section captures unserviceable control actions that can lead to hazards. These UCAs may not always lead to a hazard, but in a worse-case scenario they can. Regardless of how likely, or unlikely, it is that the UCA will occur, they are documented. This analysis does not focus on probabilities or likelihoods, it focuses on identifying a full set of UCAs so that prevention can be designed into the system. To identify UCAs, each control action was analyzed in the four ways a control action can be inadequate (Leveson, 2011):

- A control action is not provided or not followed
- An unsafe control action is provided
- A control action is provided too early, too late, or in the wrong order
- A control action is stopped too soon or applied too long

One important hazard included is the operator ignores an alarm (H-3). For the purpose of this analysis, the author defined two ways to inform an operator about operating conditions and instructions. The first method is to use an active alert. An active alert generates an indicator such as a lamp, audible tone, or a display message when a condition exists that requires different operator behavior. The second method is to provide passive information or instructions. Passive instructions do not proactively notify the operator. The operator is allowed to find the information through the operator interface after observing a condition. Passive alerts help prevent alarm fatigue by reducing the number of active alerts an operator needs to monitor and address. For example, a display page that informs the operator about the system health and instructs the operator on next steps is a passive instruction. A fuel gauge passively conveys fuel level to an operator. If a light comes on when fuel is low, the light is an active alert. These terms are referenced in the UCAs, system constraints, and requirements, so it is important the consumers of the analysis results understand the terminology used.

Two different service tasks were analyzed, cleaning the sensor and replacing the sensor. The control actions associated with these tasks and the generated UCAs are summarized in Table 14, Table 15, Table 16. This is a partial list of control actions for the entire system. The UCAs and scenarios identified by analyzing these two service tasks should generate similar system constraints and requirements for the other system service tasks.

Table 14: UCAs for TICU Control Action 1

Control Action: TICU.1 - Provide "replace sensor" instructions	
Not providing causes hazard	a1: TICU does not provide "replace sensor" DTC when sensor needs replacement. (H-4)
Providing causes hazard	b1: TICU provides "replace sensor" DTC when sensor does not need replacement. (H-1, H-2)
	b2: TICU provides "replace sensor" DTC when other DTCs related to the same problem are also provided. (H-1, H-3, H-4)
	b3: TICU provides active "replace sensor" instructions when the operator is already aware of the problem and not using TI. (H-3)
Too soon, too late, out of order	c1: TICU provides "replace sensor" DTC before sensor problem is confirmed. (H-2, H-3)
	c2: TICU provides "replace sensor" DTC too late after a sensor failure affects TI performance. (H-1)
Stopped too soon, applied too long	d1: TICU stops providing "replace sensor" DTC before sensor is replaced. (H-1, H-2, H-4)
	d2: TICU continues providing "replace sensor" DTC after sensor is replaced. (H-3, H-4)

Table 15: UCAs for TICU Control Action 2

Control Action: TICU.2 - Provide "clean sensor" instructions	
Not providing causes hazard	a1: TICU does not provide active "clean sensor" instruction when TI is disabled due to dirty sensor. (H-1)
Providing causes hazard	b1: TICU provides active "clean sensor" instruction when the sensors are not being used. (H-3, H-6)
	b2: TICU provides active or passive "clean sensor" instruction when sensor is clean. (H-1, H-6)
Too soon, too late, out of order	c1: TICU provides active "clean sensor" instruction before sensor is dirty enough to affect TI performance. (H-1, H-6)
Stopped too soon, applied too long	d1: TICU stops providing "clean sensor" instruction while sensor is dirty enough to affect TI performance. (H-1)
	d2: TICU continues to provide “clean sensor” instruction after sensor is cleaned. (H-3)

Table 16: UCAs for Service Technician Control Action 1

Control Action: ST.1 – Replace sensor	
Not providing causes hazard	a1: Service technician does not replace the sensor when sensor needs replacement. (H-2)
Providing causes hazard	b1: Service technician replaces the sensor when the sensor does not need replacement. (H-2, H-6)
	b2: Service technician damages the sensor or other components while replacing the sensor. (H-4, H-5)
Too soon, too late, out of order	c2: Service technician replaces the sensor after spending more than <X> minutes troubleshooting. (H-4)
Stopped too soon, applied too long	d1: Service technician replaces the sensor, but does not complete the repair. (for example, doesn't plug in harness). (H-2, H-4)

Each unserviceable control action generates constraints on the controller behavior, as shown in Table 17. In general, each controller constraint is the inverse of its associated UCA. This is a partial list of UCAs and controller constraints, the additional UCAs and constraints are in the STPA Details Appendix.

Table 17: Controller Constraints

Unserviceable Control Action (UCA)	**Controller Constraint**
TICU.1a1: TICU does not provide "replace sensor" DTC when sensor needs replacement. (H-4)	TICU.CC1: TICU must provide "replace sensor" DTC when sensor needs replacement.
TICU.1b1: TICU provides "replace sensor" DTC when sensor does not need replacement. (H-1, H-2)	TICU.CC2: TICU must not provide "replace sensor" DTC unless sensor needs to be replaced.
TICU.1b2: TICU provides DTC when other DTCs related to the same problem are also provided. (H-1, H-3, H-4)	TICU.CC3: TICU must provide one DTC that identifies the desired operator or service technician behavior.
	SYSTEM.CC1: The machine must not provide multiple DTCs at the same time.
TICU.1b3: TICU provides "replace sensor" DTC when the operator is already aware of the problem and is not using TI. (H-3)	TICU.CC4: TICU must only provide "replace sensor" DTC when the operator is not already aware of the problem and is using TI.
TICU.1c1: TICU provides "replace sensor" DTC before sensor problem is confirmed. (H-2, H-3)	TICU.CC5: TICU must not provide "replace sensor" DTC before sensor problem is confirmed.

TICU.1c2: TICU provides "replace sensor" DTC too late after a sensor failure affects TI performance. (H-1)	TICU.CC6: TICU must provide "replace sensor" DTC within X sec of detecting fault.
TICU.1d1: TICU stops providing "replace sensor" DTC before sensor is replaced. (H-1, H-2, H-4)	TICU.CC7: TICU must provide "replace sensor" DTC until sensor is replaced.
TICU.1d2: TICU continues providing "replace sensor" DTC after sensor is replaced. (H-3, H-4)	TICU.CC8: TICU must stop providing the "replace sensor" DTC after sensor is replaced.

4.4 STPA Step 4: Identify Loss Scenarios

This section explores why the UCAs may occur. For each UCA and control action, scenarios were generated to identify the causal factors that can lead to the UCA or hazards. The scenarios explain either why the UCA may occur or why adequate control actions may be provided, but still lead to a hazard. While identifying the "why", recommendations were generated to prevent the causal factors. These recommendations include software requirements, hardware requirements, system constraints, and design process recommendations.

The STPA handbook describes four main categories of loss scenarios (Leveson & Thomas, 2018).

Why would Unsafe Control Actions occur?

1. Unsafe controller behavior
    - Failures involving the controller (for physical controllers)
    - Inadequate control algorithm / decision-making
        - Flawed implementation
        - Specified algorithm is flawed
        - Specified algorithm becomes inadequate over time
    - Unsafe control input from another controller
    - Controller's process model does not match reality
2. Inadequate feedback and information
    - Feedback is not received
    - Inadequate feedback is received

Why would control actions be improperly executed or not executed, leading to hazards?

3. Control action not executed
    - Sent by controller, but not received by actuator
    - Received by actuator, but actuator did not respond

- Actuator responds, but control action is not applied or received by the controlled process
- Applied or received by the controlled process, but controlled process does not respond

4. Control action improperly executed
    - Sent by controller, but improperly received by actuator
    - Received by actuator, but actuator responds inadequately
    - Actuator responds adequately, but control action is applied or received improperly by the controlled process
    - Not sent by controller, but actuator responds as if it had been sent
    - Applied or received by the controlled process, but controlled process improperly responds
    - Not applied by controlled process, but process responds as if it had been applied

To explore how these loss scenarios can apply to serviceability control actions, Table 18 and Table 19 contain a physical controller and human controller example for each of the four scenario categories. These are examples of UCAs and scenarios that are common across different physical systems and could be reused in future analyses. These examples also highlight the link between elements in the control structure and how the same causal factors can affect multiple UCAs. After completing a thorough analysis of one UCA, the same loss scenarios will often apply to other UCAs expediting the analysis process.

The physical controller control action and UCA for the examples below:

Control Action: Provide "replace component" DTC

UCA: Physical process control unit (PCU) provides "replace component" DTC instruction when component does not need replacement (H-1, H-2)

The service technician (human controller) control action and UCA for the examples below:

Control Action: Replace component

UCA: Service technician replaces component when it does not need replacement (H-2, H-6)

Table 18: Common Service Scenarios – Why would UCA occur?

Scenario Type 1: Controller behavior	
Physical controller (PCU) **UCA:** PCU provides "replace component" DTC instruction when component does not need replacement (H-1, H-2)	**Service Technician (ST)** **UCA:** The service technician replaces component when it does not need replacement (H-2, H-6)
PCU Scenario 1: The controller falsely provides "replace component" DTC due to flawed DTC software logic. Requirements were missed or inadequate during system design. Example: DTC logic did not account for environmental conditions	**ST Scenario 1:** A problem occurs, and the PCU provides a DTC. The service technician replaces component when it does not need replacement, because the DTC did not specify what repair was required. The troubleshooting steps to confirm an issue with component takes longer than replacing it. The service technician replaces component, believing it is the most likely fix to the problem.
Scenario Type 2: Inadequate feedback and information	
PCU Scenario 2: The controller falsely provides "replace component" DTC because PCU incorrectly believes component needs replacement. This flawed process model will occur if: - Sensor falsely sends fault status due to sensor physical failure, Sensor power loss, Inaccuracies in sensor measurement, Sensor degradation over time - PCU incorrectly interprets missing feedback as a fault status. Feedback could be missing due to harness, connection or sensor failure - Feedback messages are corrupted	**ST Scenario 2**: The service technician replaced component when it does not need replacement because the machine provided a false "replace component" DTC. Why? See PCU Scenario 1

Table 19: Common Service Scenarios – Why would control action lead to hazard?

Scenario Type 3: Control action not executed	
Physical controller (PCU) **Control Action:** Provide "replace component" DTC instructions	**Service Technician (ST)** **Control Action:** Replace component
PCU Scenario 3: The PCU provides "replace component" DTC, but another controller provides a different DTC at the same time. The multiple DTCs are related to the same problem, but provide conflicting or misleading instructions. The service technician is unsure of the correct repair. The service technician replaces component, believing it is the most likely fix to the problem. After replacing component, the problem still exists.	**ST Scenario 3:** The PCU provides a "replace component" DTC, but the service technician does not replace component. The "replace component" DTC instructions are unclear or misleading. For example: A DTC is provided indicating a problem with a sensor circuit. The most likely repair needed is a wiring harness or connector repair, but the DTC instructions mention a sensor. The service technician replaces sensor when it doesn't need replacement due to misleading DTC instructions.
Scenario Type 4: Control action improperly executed	
PCU Scenario 4: The PCU provides the "replace component" DTC, but the service technician replaces the wrong part. Why? See ST Scenario 3.	**ST Scenario 4:** The PCU provides a "replace component" DTC, and the service technician replaces the components. However, the new component is damaged during assembly due to inadequate access.

To generate recommendations and requirements, control actions and UCAs were analyzed and causal scenarios created. For example, consider the replace sensor control action. As shown in Figure 22, the physical machine provides feedback to the service technician in the form of observable symptoms and DTCs to indicate a problem with the sensor. DTC instructions are provided to the service technician as a control, instructing the technician to replace the sensor. The service technician then repairs the physical machine by replacing the component.

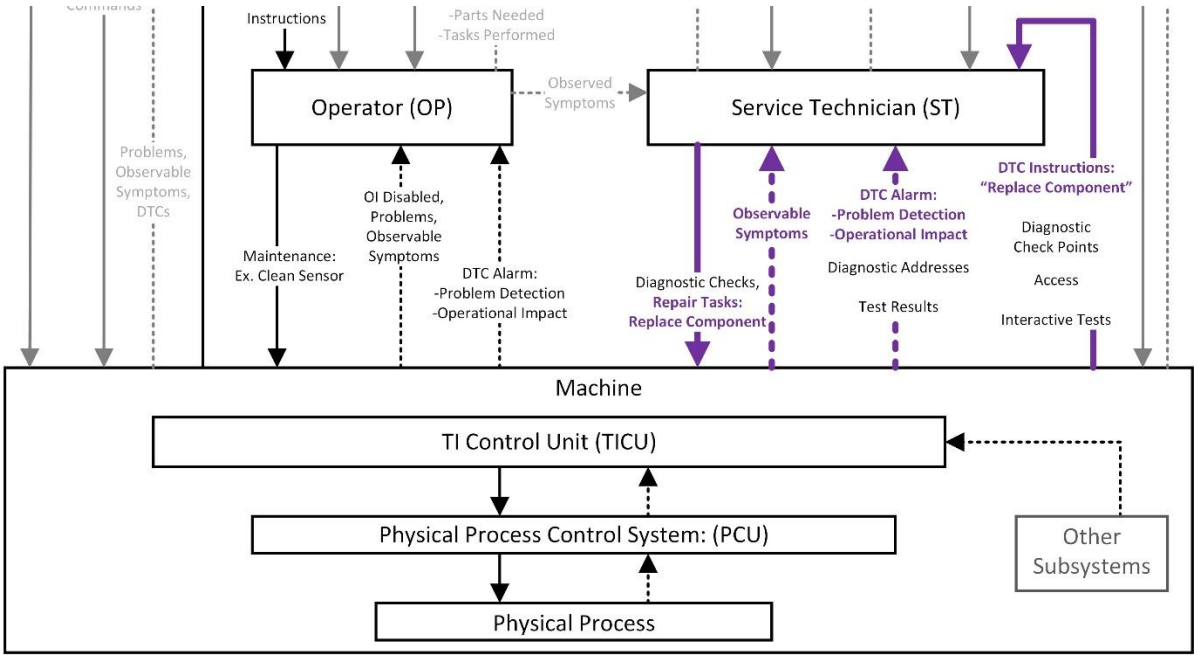

Figure 22: Replace Sensor Control Actions

Control Action - TICU.1: Provide "replace sensor" instructions

Scenario 1: The TICU does not provide "replace sensor" DTC when sensor needs replacement [TICU.1a1]. TI system is disabled per functional constraints, but neither the operator nor service technician know why the system is disabled or what to do to resolve the problem. The TICU may incorrectly believe that the sensor is OK, therefore the TICU does not send the DTC. This may happen because:

TICU.1a1.CS:

a) The physical TICU controller failed.
b) The TICU "replace sensor" DTC algorithm is inadequate due to flawed specifications or flawed implementation.
c) The TICU "replace sensor" DTC algorithm becomes inadequate over time due to hardware changes.
d) Sensor fault status is missing due to physical sensor failure, harness failure, or unplugged harness.
e) The sensor status signal is stuck on OK, when sensor is actually faulted.
f) Sensor sends incorrect feedback indicating sensor is OK, when it's actually faulted due to flawed specifications.

g) TICU receives the faulted status signal but misinterprets it or ignores it because the message is corrupted or compromised.
h) The TICU does not receive the faulted status signal because the communication network is overloaded.
i) The sensor fault status feedback does not exist due to flawed specifications or flawed implementation.

Potential recommendations and requirements generated based on scenario 1 include:

Design Process Recommendations:

- Design Process: A sensing system design review must be conducted on the sensors to ensure correct thresholds and threshold tolerances. (TICU.1a1.CSb)
- Design Process: TICU DTC software must be complete before field testing. (TICU.1a1.CSb), (TICU.1a1.CSh)
- Design Process: Frequently occurring DTCs identified during field testing must be investigated and addressed before production. (TICU.1a1.CSb)
- Design Process: The design process must require and enforce software compatibility reviews if service part hardware changes post production. Software must be compatible with all service part hardware versions. (TICU.1a1.CSc)
- Design Process, TI System Design: The sensor design and fault status feedback algorithm must be reviewed by the design teams and the supplier. If the sensor can't detect specific problems, the TICU system must be designed to accommodate the limitation and ensure the TICU can detect the problem. (TICU.1a1.CSf)

Testing Process Recommendations:

- Testing Process: Field testing must report inadequate or ineffective DTCs. (TICU.1a1.CSb)
- Testing Process: DTC occurrences must be tracked during field testing. (TICU.1a1.CSb)
- Testing Process: Product test must measure and verify controller processor tasks times to ensure there is no overrun. (TICU.1a1.CSh)
- Testing Process: Product test must verify maximum communication network load requirement. (TICU.1a1.CSh)

Design Requirements:

- Product Design: The product must detect TICU controller failures. (TICU.1a1.CSa)
- TI System Design: The TI system must be capable of detecting a sensor physical failure. (TICU.1a1.CSi)

- TI System Design: The TI system must be capable of differentiating a harness or connector problem from a sensor failure. (TICU.1a1.CSd)
- TI System Design: The TI system must provide sensor fault status feedback to the TICU. (TICU.1a1.CSi)
- TI System Design, Software: The TICU must provide a "check sensor connection" DTC if a harness or connector problem is detected. (TICU.1a1.CSd)
    - Assumption: TICU can't differentiate between a harness failure, connector failure, or unplugged connector.
- TI System Design, Software: The TICU system must periodically conduct a self-check. (TICU.1a1.CSe)
- TI System Design, Software: The system must detect corrupted messages. (TICU.1a1.CSg)
- TI System Design, Software: The software must monitor to make sure controller processor tasks are running properly. (TICU.1a1.CSh)

Technical Information Requirements:

- TI TM: "Check sensor connection" DTC must have adequate diagnostic instructions in the TM to identify the correct repair needed. (TICU.1a1.CSd)
- TI TM: "Check sensor connection" DTC diagnostic instructions must cover all possible repairs (unplugged, harness repair, connector repair). (TICU.1a1.CSd)

Over-alerting operators is a serious problem in complex machinery. While running a piece of equipment, operators must monitor and respond to various alarms meant to inform the operator about system performance and problems. DTCs contribute to operator alarm fatigue when they falsely indicate a problem, when they don't clearly and effectively communicate the operator action required, and when multiple DTCs trigger at the same time. The following UCA analyzed demonstrates how STPA methodology can be used to generate system design requirements to prevent operator fatigue.

Control Action - TICU.1: Provide “replace sensor” instructions

Scenario 2: TICU provides "replace sensor" DTC when the operator is already aware of the problem and is not using TI. [TICU.1b3]. The TICU provided the DTC when a problem was detected. The operator decides to continue running without TI and disables the system. However, the DTC is redisplayed, and the operator is annoyed by the notification and immediately dismisses the alarm. The unhelpful alarm contributes to operator alarm fatigue and degrades the effectiveness of future alarms. This may happen because:

TICU.1b3.CS:

a) After taking a break and shutting down the machine, the DTC reappears on startup due to flawed DTC specifications or implementation.
b) The DTC reappears after the operator disables TI and continues running due to flawed DTC specifications or implementation.
c) The physical controller failed sending a false DTC. (similar to TICU.1a1.CSa)
d) The sensor fault status signal intermittently disappears and reappears, retriggering the DTC. The intermittency is due to a loose connector, faulty wiring harness, or other intermittent circuit fault.
e) The sensor fault status is continuously sent, but the TICU does not receive it because the communication network is overloaded. The DTC condition times out, resolving the DTC. Once the TICU processor tasks catch up, the DTC is triggered. (similar to TICU.1a1.CSh)

Potential development process recommendations and system design requirements based on scenario 2 include:

Design Process Recommendations:

- Design Process: All TI DTC instructions must be reviewed by a cross functional team to ensure effective customer-facing language and communication. (TICU.1b3.CSb)
- Design Process: All TI DTC active alarms must be reviewed by a cross functional team to ensure appropriate alarm severity level. (TICU.1b3.CSb)

Design Requirements:

- TI System Design, Software: The "replace sensor" active alarm must not trigger while TI is disabled. (TICU.1b3.CSa)
- TI System Design, Software: The "replace sensor" active alarm must not trigger unless the sensor needs to be replaced to continue using TI. (TICU.1b3.CSa)

- TI System Design, Software: If TI is disabled because the sensor needs to be replaced, the system must provide feedback to the operator that TI is disabled and cannot be re-enabled until the system is serviced. (TICU.1b3.CSa)
    - Assumption: TI system will be disabled if the sensor needs to be replaced per functional constraints.
- TI System Design, Software: The system should provide passive information about TI disabled status and what to do about it. (TICU.1b3.CSa)
- TI System Design, Software: While the DTC is active, the DTC active alarm must not be redisplayed in the same key cycle. (TICU.1b3.CSb)
- TI System Design, Software: If the DTC occurs, resolves and reoccurs within the same key cycle, it must not actively re-alarm the operator unless the operator turns on TI. (TICU.1b3.CSd)
- TI System Design, Software: The "replace sensor" DTC algorithm must wait > X sec to resolve DTC after sensor OK status is received. (TICU.1b3.CSd)
    - Assumption: Waiting X sec won't impact the machine operation.

This case study demonstrated that STPA methodology can apply to design for serviceability. Analyzing two UCAs identified ten recommendations for the development process and sixteen design requirements for the physical system, software, and technical information. Additional scenarios and recommendations are included in the STPA Details Appendix. This technique provides a methodical way to design for emergent properties and generate system constraints and design requirements. Additional conclusions and insights on applying STAMP techniques to serviceability are discussed in section 5.

5 Recommendations and Conclusions

5.1 Applying STAMP to Serviceability

The purpose of this research was:

"To improve product serviceability by identifying systems-theory based methods for generating serviceability requirements and recommendations using STAMP techniques."

This research is important because of the increasing cost and impact of machine unavailability. Labor shortages, increasing labor rates, and increasing equipment size and cost contribute to the urgent need for improved equipment serviceability. When the machine is being serviced, it's unavailable. The opportunity cost of lost productive time plus the cost of service impacts the customer's profitability. Customers expect equipment to be available when they need it.

Machine complexity is rapidly increasing, making it more difficult to operate, service, and design. This rapid change in complexity, requires system based methods to ensure product design and post-production support meet customer needs. Emergent properties are especially hard to consider during product development. Constraints to prevent undesired system behavior are often missed due to insufficient methods of identifying system level interactions. In recent years, STAMP has risen as an effective process for managing safety. This research explored how STAMP can also be leveraged for serviceability as an emergent property. Key questions the research sought to answer include:

- As STPA and CAST are more frequently applied across the industry for safety analyses, can similar techniques be used to improve product serviceability?
- Can STAMP techniques effectively generate hardware and software serviceability requirements? Can they generate recommendations for the larger sociotechnical system including the product development process?
- If STPA can be applied to serviceability, are any analysis modifications are required?

The CAST and STPA case studies successfully demonstrated STAMP application to serviceability. Each case study generated serviceability design recommendations. They also identified recommendations for the higher level service control structure, such as the design and test processes. The case studies created a set of service losses, hazards, control structures, and responsibilities that can be referenced and reused in future serviceability analyses.

The service analysis identified a wide range of causal factors that may contribute to inadequate serviceability. As compared to traditional hazard analyses that focus on hardware failures, both case

studies generated software and hardware requirements. They also generated service information recommendations to help drive the desired operator and technician service actions. The STPA case study was conducted on a system in an early, conceptual design phase. Few details about the system were known at the time of the analysis, yet the study effectively generated requirements and constraints to guide the system design.

Over-alarming the operator is a serious issue on complicated machinery, and service alarms contribute to operator alarm fatigue. The STPA case study addressed operator alarm fatigue as a hazard and identified scenarios that could lead to operators ignoring alarms. Traditional reliability-based analysis techniques, such as service FMEAs and reliability centered maintenance, do not consider the human in the analysis. They miss important design requirements to prevent alarm fatigue. The STPA case study demonstrated how to include the human in the service analysis.

Overall, the CAST and STPA methodologies are the same whether applying them to safety or serviceability. The key to adapting the methods to serviceability is identifying serviceability losses and hazards that follow Leveson's definitions. Per Leveson, losses may include any loss that is unacceptable to the stakeholders. A hazard is a system state or set of conditions that, together with worst-case environmental conditions, will lead to a loss (Leveson, 2011). The losses and hazards identified in these case studies are summarized below. They can be reused in future serviceability analyses.

Losses:

- Unplanned downtime due to inadequate serviceability (L-1)
- Financial losses incurred through warranty costs (L-2)
- Customer dissatisfied (L-3)

Hazards:

- Operator takes the wrong action to mitigate a problem. (L-1, L-3)
- Service technician does the wrong repair. (L-1, L-2, L-3)
- Operator ignores a service alarm. (L-1, L-3)
- Repair & troubleshooting time exceeds <X> minutes. (L-1, L-2, L-3)
- Service task introduces subsequent problems. (L-1, L-2, L-3)
- Scheduled maintenance time exceeds <X> minutes over first <X> hours of use. (L-3)

5.2 Alignment Between Safety and Service

Limited engineering resources and aggressive product development timelines drive the need for more efficient product development processes. Aligning stakeholder needs can reduce coordination efforts and help optimize design trade-off decisions. A secondary objective of this research was to explore leveraging and reusing safety STPA elements in a serviceability STPA as a way to improve product development efficiency. A secondary question the research sought to answer was:

- Can safety STPA control structures be reused and leveraged for serviceability, reducing engineering effort to design for serviceability?

As shown in Figure 10 and Figure 18 the general hierarchical control structures between a safety control structure and a service control structure are very similar at the top layers. Both rely on development processes to enforce the desired system behavior and feedback loops to verify control effectiveness. However, the bottom physical process control level is different between safety and service. The service physical level is less functional than the safety control structure. For example, in a safety control structure, the operator engages or disengages a system. In a service control structure, the operator maintains the system by checking the oil level. In general, the bottom level of the control structure needs to be reviewed and adapted for service.

One interesting overlap between safety and service is the operator's responsibility to monitor and respond to alarms. Operators must manage all types of alarms, including safety, service, and operational alarms. To drive desired operator behavior and avoid operator alarm fatigue, all alarm types must be considered during system development. STAMP methodologies enable system thinking when developing alarms and other operator interfaces.

Another opportunity for alignment between safety and service occurs when automatic lockouts or shutdowns are designed into the system to prevent damage. The feedback required to apply the automatic lockout often aligns with the feedback required to detect that service is required. Automatic lockout and shutdown software requirements may be generated through a safety or a service analysis. The associated operator alarms should drive the desired operator behavior which includes operating the machine in a different manner and servicing the machine.

5.3 Other Insights and Recommendations to Improve Serviceability

This research generated several insights on how to improve serviceability. First of all, thinking about service instructions as a method to drive desired operator and service technician behavior may lead to more effective service instructions. It is the author's observation that service information often focuses

on identifying “root causes” instead of instructing the operator or technician. The design team cares about a lower level of causal factors than the service technician. This can lead to service information that isn’t optimized to operator and technician needs. For example, if a component stops working, the product development team needs to know why so design changes can be made. If the component isn’t repairable, the service technician just needs to replace the component. Conflicting stakeholder needs can contribute to “dual-purposed” service information that isn’t optimized for the customer. Designing service information as a control to drive desired customer behavior may avoid this scenario.

One recommendation is simply referring to service alarms in a different manner. Describe alarms by the desired action instead of by the condition detected. For example, in the STPA case study the author referred to the “replace component” DTC, instead of the “component fault” DTC. Thinking about the control action may identify service alarms with missing instructions and help optimize what type of feedback the operator and the service technician needs. There may be times when the operator is allowed to observe a condition without an active alarm, then do the service task themselves or call for service support. The STPA case study provides an example. If the operator can observe a dirty sensor, they will do the desired behavior (clean the sensor) without an active alarm. The operator will clean it when it becomes a problem for them. If the operator can’t observe the dirty sensor, an active service alarm may be appropriate.

The CAST case study highlighted another example. A low supply pressure service alarm DTC existed to indicate a problem. However, there were no service instructions associated with the alarm to let the operator and service technician know why they should care about the condition and what to do about it. The DTC focused only on providing feedback instead of instructing the operator and service technician. Describing service alarms by the control action has two key benefits. It may improve service instructions, and it may reduce operator alarm fatigue by improving service alarm effectiveness.

The case studies demonstrated that defining controller responsibilities, process/mental models, and feedbacks is a powerful method to generate service feedback requirements. The STPA case study highlights two key aspects of this process. Defining the desired service actions and the targeted human controller (for example, the operator or service technician), identifies the feedback they need to choose the correct action. This is powerful because it produces software, hardware, and service instruction requirements at the same time. Considering the whole system helps avoid a disjointed service experience that may emerge when software, hardware, and service instructions are each created in development silos.

Applying the same process to physical controllers is the second key aspect. After analyzing the operator and service technician, the process can be applied one level down to generate more detailed

design requirements. Here's an example from the STPA case study. To drive the desired service technician behavior of replacing the sensor, the analysis identified a requirement for a "replace sensor" service DTC. Applying the same process to the "replace sensor" DTC, identified the feedback needed for the machine to automatically decide that the sensor needs replacement. This incremental process can be applied in early, conceptual design phases to guide a service-friendly system design.

Another key finding from the CAST study is the need for product development metrics and incentives that provide a holistic view of machine availability. Developing products that are built to last is critical. However, they must also be serviceable, so that when problems do occur, they can be resolved quickly. Reliability has been a focus area since the early 1900's, while serviceability is a much newer focus area (de Weck et al., 2012). Historically, when machines were easier to service and skilled technicians were more readily available, reliability may have been the most important product element of machine availability. For today's complex machines, a reliability-only view of machine availability does not fully capture customer needs. To optimize machine availability for the customer, metrics that include reliability and serviceability are needed to drive design decisions and solutions that meet customer expectations.

The author recommends that STPA is adopted as a "design for" serviceability method. Both case studies demonstrate that systems-theory based methods effectively generate system service constraints and design requirements. It is the author's hope that the recommendations generated in the case studies are applied to improve supply pressure system diagnostics and influence TI system future design. The case study recommendations are detailed in sections 3.7 and 4.4.

This research demonstrated that STAMP can be applied to serviceability, whether using it to address existing issues or to "design for" future systems in early design phases. Service STPA is an effective method for generating hardware and software design requirements for complex systems. In addition, the analyses produced recommendations for the product development and support processes. Processes are often left out of traditional analysis techniques, but robust system development and operational support are critical to meet demanding stakeholder needs. By using STAMP techniques to understand system interactions and strengthen service control structures, OEMs can address many of the challenges they are currently facing providing machine serviceability and service support.

6 Bibliography

Ball, A. J. (2015). *Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development*. Massachusetts Institute of Technology.

Barkai, J. (1999). Automatic Generation of a Diagnostic Expert System from Failure Mode and Effects Analysis Information. *SAE Technical Papers*, *01–0060*.

Blanchard, B. S., Verma, D. C., & Peterson, E. L. (1995). *Maintainability: A Key to Effective Serviceability and Maintenance Management*. John Wiley & Sons.

Bowles, J. B. (2003). Fundamentals of Failure Modes and Effects Analysis. *Tutorial Notes Annual Reliability and Maintainability Symposium*. Tampla, FL.

de Weck, O. L., Ross, A. M., & Rhodes, D. H. (2012). Investigating Relationships and Semantic Sets amongst System Lifecycle Properties (Ilities). *3rd International Engineering Systems Symposium*. Retrieved from http://hdl.handle.net/1721.1/102927

Dyadem Press. (2003). *Guidelines for failure mode and effects analysis for automotive, aerospace, and general manufacturing industries*. CRC Press.

Erickson, B., Fausti, S., Clay, D., & Clay, S. (2018). Knowledge, Skills, and Abilities in the Precision Agriculture Workforce: An Industry Survey. *Agronomy, Horticulture and Plant Science Faculty Publications*, *57*. Retrieved from https://openprairie.sdstate.edu/plant_faculty_pubs/57/

Goble, W. M., & Brombacher, A. C. (1999). Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. *Reliability Engineering and System Safety*, *66*(2), 145–148. https://doi.org/10.1016/S0951-8320(99)00031-9

Goerges, S. L. (2013). *System theoretic approach for determining causal factors of quality loss in complex system design* (Massachusetts Institute of Technology). https://doi.org/10.1115/DETC201434156

Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N. G. (2019). *CAST Handbook*. Retrieved from http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook*. Retrieved from http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Montes, D. R. (2016). *Using STPA to Inform Developmental Product Testing*.

Moubray, J. (1997). *Reliability Centered Maintenance* (Second Ed.). Industrial Press Inc.

Nowlan, F. S., & Heap, H. F. (1978). *Reliability-Centered Maintenance*. Washington, D.C.

Pecht, M. (Ed.). (2009). *Product reliability, maintainability, and supportability handbook* (Second ed.). CRC Press.

Rhee, S. J., & Ishii, K. (2003). Using cost based FMEA to enhance reliability and serviceability. *Advanced Engineering Informatics*, *17*(3–4), 179–188.

Society of Automotive Engineers International. (2002). A guide to the reliability-centered maintenance (RCM) standard. SAE JA1012.

Society of Automotive Engineers International. (1999). Evaluation Criteria for Reliability-Centered Maintenance (RCM) Process. SAE JA1011.

US MIL-STD-1629: Procedures for performing a failure mode, effects and criticality analysis. (1980).

Walden, D. D., Roedler, G. J., Forsberg, K., Hamelin, R. D., & Shortell, T. M. (2015). *INCOSE Systems Engineering Handbook : A Guide for System Life Cycle Process* (Fourth ed.). Retrieved from http://web.b.ebscohost.com.libproxy.mit.edu/ehost/detail/detail?vid=0&sid=8079ff2b-fb52-48db-b08e-87b2d148e675%40pdc-v-sessmgr06&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=1016324&db=nlebk

Young, W., & Leveson, N. (2013). Systems thinking for safety and security. *Proceedings of the 29th Annual Computer Security Applications Conference*, 1–8. https://doi.org/10.1145/2523649.2530277

Young, W., & Leveson, N. G. (2014). Inside risks an integrated approach to safety and security based on systems theory: Applying a more powerful new safety methodology to security risks. *Communications of the ACM*, *57*(2), 31–35. https://doi.org/10.1145/2556938

7 Appendix: Service CAST Details

7.1 System Responsibilities

This section contains the additional system element responsibilities not included in section 3.4.1.

Table 20: Service Responsibilities - Physical Process (PP)

General Responsibilities	Specific
Provide manual monitoring features to operators and service technicians (example: visual oil level gauge)	X
Protect the system from damage	
Provide manual diagnostic check points such as diagnostic ports & receptacles	X
Provide adequate access to perform service tasks	

Table 21: Service Responsibilities - Dealer/Service Shop (SS)

General Responsibilities	Specific
Resolve problems quickly to minimize customer downtime	X
Provide operator training	
Provide service technician training	X
Provide work instructions for service technicians	X
Remotely monitor machine health	
Receive service requests from customers, provide support to customers, and dispatch service technicians	
Provide real-time technical assistance to field service technicians	X
Request service support as needed (Call manufacturer TAC)	
Communicate observed symptoms and service actions taken	
Identify parts needed for a repair	
Order and provide parts needed for a repair	
Bill out service charges	
Submit warranty data to manufacturer	

Table 22: Service Responsibilities - Farm Operation (FO)

General Responsibilities	Specific
Keep equipment running	
Remotely monitor equipment alarms	
Provide operator training	X
Provide work instructions to operators	
Ensure equipment is being operated in a way that does not lead to machine damage	
Ensure equipment is properly maintained	
Receive problem reports and service requests from operators	
Request service support as needed (call a dealer/service shop)	
Communicate observed symptoms and service actions taken	

Table 23: Service Responsibilities –Product Design (PD)

General Responsibilities	Specific
Design for service to minimize downtime	X
Quick and easy to diagnose	X
Quick and easy to repair	
Quick and easy to maintain	
Avoid special service tools	
Provide monitoring to predict failures and prevent damage when problems occur	
Develop service alarms (DTCs) that drive desired operator and technician behavior	X
Follow development process	X
Meet stakeholder needs	
Monitor problem reports and change requests	
Make design changes to address problems (pre and post production)	
Communicate continuous improvement design changes to product support	
Document design information, rationale, and assumptions	X
Learn from past serviceability problems and improve design based on feedback	X
Follow service standards and adhere to regulations	

Table 24: Service Responsibilities – Product Test (PT)

General Responsibilities	Specific
Verify system meets requirements	X
Validate emergent behavior meets serviceability needs	X
Conduct tests	
Operate and service test equipment	
Ensure real or representative service and operating environments during testing	X
Document and communicate service problem reports, test reports, and change requests	X

Table 25: Service Responsibilities – Industry Standards and Regulations (SR)

General Responsibilities	Specific
Develop design for serviceability standards	X
Develop service support standards	
Develop and enforce regulations	

7.2 Component Analysis

This section contains the additional system element analysis not included in section 3.5.2.

Operator (OP)

Service-Related Responsibilities

- OP.R-1: Maintain the equipment: Check and maintain hydraulic oil level
- OP.R-2: Respond to problems that occur: Follow DTC and operator manual instructions

Control Actions Contributing to the Hazard

- OP.CHS-1: Operator did not check MG oil level when alarmed to low supply pressure. (OP.R-1, OP.R-2)
- OP.CHS-2: Operator did not respond to the correct DTC. (OP.R-2) This contribution was not confirmed in the data available. However, this is a common CHS when multiple DTCs trigger at the same time. The author assumed worse case conditions.

Why? Process/Mental Model Flaws

- OP.F-1: Operator didn't know that low oil level could cause the low pressure DTC. DTC did not tell the operator to check oil level. (OP.CHS-1)
- OP.F-2: Operator thought oil level was OK. (OP.CHS-1)
- OP.F-3: Missing information to direct the operator to the action required. (OP.CHS-2)

Why? Contextual Factors

- OP.F-4: Harvest is a high pressure, rushed time of year. Operator will do whatever they think is fastest to keep the machine running. (OP.R-1)
- OP.F-5: When a service alarm doesn't issue a specific operator control action, operators will typically ignore the alarm or call for service support. (OP.R-1, OP.R-2)

Dealer/Service Shop (SS)

Service-Related Responsibilities

- SS.R-1: Resolve problems quickly to minimize customer downtime
- SS.R-2: Provide service technician training
- SS.R-3: Provide work instructions for service technicians
- SS.R-4: Provide real-time technical assistance to service technicians

Control Actions Contributing to the Hazard

- SS.CHS-1: Did not ensure adequate time was spent diagnosing before replacing parts. (SS-R.1)

Little information is known about the service shop actions. Questions are captured below that would need to be answered to generate further recommendations for the dealer/service shop.

- *Question: What training was provided on servicing electrical and hydraulic systems? What training was provided specific to this equipment and system?*
- *Question: What work instructions were provided for this system or DTC?*
- *Question: What real-time technical assistance was provided to service technicians? Were system experts available as resources?*
- *Question: If a system expert was available, were they assigned to this problem? If not, why?*

Why? Process/Mental Model Flaws

- Unknown

Why? Contextual Factors

- SS.F-1: Harvest is a critical and rushed time of year. When machine problems happen, customers are dissatisfied and need the equipment up and running as fast as possible. Unplanned service is a high pressure situation. (SS.CHS-1)
- SS.F-2: The responsibility to resolve problems quickly can directly conflict with the responsibility to ensure adequate time is spent diagnosing. (SS.CHS-1)
- SS.F-3: Service technician time spent diagnosing shifts scarce resources away from more profitable business opportunities. (SS.CHS-1)

- SS.F-4: When costs are covered by warranty, there's little incentive to restrict part costs. (SS.CHS-1)
- SS.F-5: It can be difficult to bill out for diagnostic time. Customers expect service technicians to figure out what repair is required quickly. (SS.CHS-1)
- SS.F-6: During peak work seasons, there's often more jobs to do than people available to cover them. Agriculture is a cyclical industry with busy times during planting and harvesting season and less busy times in the winter. (SS.CHS-1)
- SS.F-7: Due to industry service technician shortage, it can be difficult to find qualified service technicians to hire. (SS.CHS-1)

Farm Operation (FO)

Service-Related Responsibilities

- PO.R-1: Provide operator training

Control Actions Contributing to the Hazard

Little information is known about the service shop actions. Questions are captured below that need to be answered to generate further recommendations for the farm.

- *Question: What training was provided on checking and maintaining oil level? Did training include explanation of two reservoirs?*
- *Question: What training did the farm operation receive from the equipment dealer/service shop on checking and maintaining oil level as part of regular maintenance?*

Why? Process/Mental Model Flaws

- Unknown

Why? Contextual Factors

- Harvest is a critical and rushed time of year. Downtime can be a high pressure situation.
- Skilled operators are increasingly difficult to hire due to labor shortages.

Product Design (PD):

Service-Related Responsibilities

- PD.R-1: Design for service to enable quick and easy diagnostics (SC-5, SC-7, SC-10, SC-11)
- PD.R-2: Develop DTCs that drive desired operator and technician behavior (SC-3, SC-4, SC-8, SC-9)
- PD.R-3: Follow design process (SC-10)
- PD.R-4: Document design information, rationale, and assumptions (SC-6)
- PD.R-5: Learn from past serviceability problems and improve design based on feedback (SC-10)

Control Actions Contributing to the Hazard

- PD.CHS-1: PD contribution 1. (PD.R-1)
- PD.CHS-2: Designed DTCs that drove undesired operator and technician behavior. (PD.R-2)
- PD.CHS-3: PD contribution 3. (PD.R-3)
- PD.CHS-4: PD contribution 4. (PD.R-4)
- PD.CHS-5: PD contribution 5. *(Question: Was cross functional team involved in the diagnostic design? If no, why not? [PP.F-7])* (PD.R-5)

Why? Process/Mental Model Flaws

- PD.F-1: Product design believed the DTC design was sufficient. Inadequate feedback on DTC effectiveness. (PD.CHS-2) (*Question: Why was DTC feedback? [PT.CHS-1, PT.CHS-2]. [PS.F-7]*)
- PD.F-2: Assumed adequate knowledge transfer between development groups. (PD.CHS-4)

Why? Contextual Factors

The following contextual factors already identified apply:

- PP.F-4: Program metrics. (PD.CHS-1, PD.CHS-3)
- PP.F-6: Legacy system evolution. (PD.CHS-1)
- PP.F-7: Development process and guidelines. (PD.CHS-4, PD-CHS.5)

Additional contextual factors include:

- PD.F-3: Missing DTC requirements to account for system interactions and behavior. Inadequate understanding of system behavior and interactions.
- PD.F-4: System complexity rapidly increased, affecting human ability to understand how the system works. It was easy to miss system level requirements, interfaces, and interactions. The complexity made emergent behavior more difficult to predict and "design for." System

development required collaboration between the electrical team, software team, hydraulic team, and propulsion team to capture all of the subsystem interfaces. Responsibility for interfaces and emergent properties were not clearly defined by processes.

- PD.F-5: The system complexity increased over time reducing diagnosibility. The past system was easier to diagnose due to less functions on the same circuit. Underestimated increased system complexity in program scope and resource planning. (PD.CHS-1, PD.CHS-2)
- PD.F-6: Inadequate design documentation resources, processes, and tools to ensure adequate information was available for product support to create technical instructions and training content. (PD.CHS-4)
- PD.F-7: Prioritized cost and other stakeholder needs over diagnosibility. Cost pressures prevented adding additional sensing and self-diagnostic capabilities. (*Question: Why? [PP.F-4])*
- PD.F-8: DTCs were not always included or finalized in pre-production software versions, missing the opportunity to test on physical machines. Lack of management commitment to ensure diagnostics are complete before field testing. (PD.CHS-2)
- PD.F-9: Inadequate engineering resources were available to rigorously design for diagnostics within the project timeline. (PD.CHS-1, PD.CHS-2, PD.CHS-3, PD.CHS-4, PD.CHS-5). (*Question: Did program resource calculators adequately predict electrical and software engineering needs? [Unknown])*
- PD.F-10: It was difficult to keep up with staffing needs. Electrical and software content was rapidly increasing. (All PD CHS)
- PD.F-11: No high level diagnostic goals or expectations were communicated to product design. (PD.CHS-1, PD.CHS-2) (*Question: Why? [PP.F-4, PP.F-7])*
- PD.F-12: Product design team was incentivized through reliability goals to design out problems and prevent part failures. This drove a reliability-focused view of machine availability, instead of a more holistic view that incorporates aspects of dependability and serviceability. (PP.F-7)

Product Test (PT)

Service-Related Responsibilities

- PT.R-1: Verify system meets requirements (SC-10)
- PT.R-2: Validate emergent behavior meets serviceability needs (SC-10)

- PT.R-3: Document and communicate service problem reports, test reports, and change requests (SC-10)
- PT.R-4: Ensure real or representative service and operating environments during testing (SC-10)

Control Actions Contributing to the Hazard

- PT.CHS-1: Problem reports focused on failures. (PT.R-3)
- PT.CHS-2: Inadequate testing on production intent DTC software. (PT.R-1)
- PT.CHS-3: Did not ensure representative service environments for testing serviceability. Did not leverage production-intent diagnostic information and tools to diagnose problems. (PT.R-4)
- PT.CHS-4: Inadequate validation of serviceability. (PT.R-2)

Why? Process/Mental Model Flaws

- PT.F-1: Assumed the problem would be designed out before production, and therefore the service technician won't struggle with diagnostics in the same way. (PT.CHS-4)

Why? Contextual Factors

The following contextual factors already identified apply:

- PP.F-4: Program metrics. (PT.CHS-2)
- PP.F-7: Development process and guidelines. (PS.CHS-1, PS.CHS-3, PS.CHS-4)
- SS.F-2: Conflicting responsibility to resolve problems quickly and ensure representative service technician experience when resolving problems. (PS.CHS-3)

Additional contextual factors include:

- PT.F-2: Unclear responsibilities. (PT.CHS-1, PT.CHS-3, PT.CHS-4)
- PT.F-3: PT contextual factor 3. (PT.CHS-1)
- PT.F-4: Test engineers and test technicians were used to ignoring and dismissing DTCs. (PT.CHS-1, PT.CHS-2)
- PT.F-5: During testing priority was put on testing and designing out unexpected problems. This shifted focus away from testing and improving system diagnostics. (PT.CHS-1)
- PT.F-6: Time pressures to get the machine back up and running quickly. It was often faster to call an engineer who designed the system to help diagnose problems than to use the technical information. (PS.CHS-3)
- PT.F-7: The test engineer and test technician are typically experts on the equipment and have more system specific knowledge than the average technician. Test engineers and technicians

may be able to diagnose problems faster, and not recognize inadequate diagnostics. (PT.CHS-1, PT.CHS-3)

- PT.F-8: PT contextual factor 8.. (PT.CHS-3)
- PT.F-9: Test equipment was outfitted with many sensors and data monitoring. It was faster to use this information to diagnose problems than to use the data available through diagnostic addresses and diagnostic tools. (PT.CHS-3)

Management (MT)

Service-Related Responsibilities

- MT.R-1: Define and track metrics to drive decisions that optimize machine availability (SC-10)
- MT.R-2: Define and enforce serviceability controls within the design process (SC-10)
- MT.R-3: Define serviceability standards, design guidelines, and analysis techniques (SC-10)

Control Actions Contributing to the Hazard

- MT.CHS-1: Inadequate metrics to optimize machine availability. (MT.R-1)
- MT.CHS-2: MT contribution 2. (MT.R-2)
- MT.CHS-3: MT contribution 3. (MT.R-3)

Why? Process/Mental Model Flaws

- MT.F-1: Reliability was most important element of machine availability and what customers want most. (MT.CHS-1)
- MT.F-2: Product diagnosibility was adequate. (MT.CHS-2, MT.CHS-3)
- MT.F-3: Assume adequate design information. (MT.CHS-3)

Why? Contextual Factors

The following contextual factors already identified apply:

- SS.F-2: Conflicting responsibility to resolve problems quickly and ensure adequate diagnostics before replacing parts. (MT.CHS-2)
- ST.F-12: System complexity rapidly increased, reducing human ability to understand how the system works. (MT.CHS-2, MT.CHS-3)
- PD.F-5: System complexity increased over time reducing diagnosibility. (MT.CHS-2)

Additional contextual factors include:

- MT.F-4: Historically, serviceability focused on maintenance and repair. This was adequate when systems were primarily mechanical and less complex. The rapid increase in system complexity, electronics, and software increased the need to deliver product diagnostic capability. (MT.CHS-1, MT.CHS-2, MT.CHS-3)
- MT.F-5: Inadequate feedback on diagnostics. (MT.CHS-1, MT.CHS-2, MT.CHS-3)
- MT.F-6: Inadequate feedback from design teams. (MT.CHS-3)

8 Appendix: Service STPA Details

8.1 UCAs and Controller Constraints

This section contains the additional controller constraints not included in section 4.3.

Table 26: Controller Constraints - continued

Unserviceable Control Action (UCA)	**Controller Constraint**
TICU.2a1: TICU does not provide active "clean sensor" instruction when TI is disabled due to dirty sensor (H-1)	TICU.CC9: TICU must provide active "clean sensor" instruction if TI is disabled due to dirty sensor
TICU.2b1: TICU provides active "clean sensor" instruction when the sensors are not being used. (H-3, H-6)	TICU.CC10: TICU must not provide active "clean sensor" instruction if TI is not turned on.
TICU.2b2: TICU provides active or passive "clean sensor" instruction when sensor is clean. (H-1, H-6)	TICU.CC11: TICU must not provide active or passive "clean sensor" instruction when sensor is clean.
TICU.2c1: TICU provides active "clean sensor" instruction before sensor is dirty enough to affect TI performance. (H-1, H-6)	TICU.CC12: TICU must only provide active "clean sensor" instruction if TI is disabled due to dirty sensor
TICU.2d1: TICU stops providing "clean sensor" instruction while sensor is dirty enough to affect TI performance. (H-1)	TICU.CC13: TICU must not stop providing "clean sensor" instruction while sensor is dirty enough to affect TI performance.
TICU.2d2: TICU continues to provide “clean sensor” instruction after sensor is cleaned. (H-3)	TICU.CC14: TICU must stop providing “clean sensor” instruction once sensor clean enough to not affect TI performance.
OP.1a1: Operator does not clean the sensor when it's dirty. (H-1)	OP.CC1: The operator must clean the sensor when it's dirty.
OP.1b1: Operator has to clean sensor too often when machine needs to be running. (H-7)	OP.CC2: The operator must not have to clean the sensors so often it creates downtime or customer dissatisfaction.
OP.1d1: Operator damages the sensor while cleaning it. (H-5)	OP.CC3: The operator must not damage the sensor while cleaning it.
ST.UCA1a1: Service technician does not replace the sensor when sensor needs replacement. (H-2)	ST.CC1: Service technician must replace the sensor when the sensor needs replacement.

ST.UCA1b1: Service technician replaces the sensor when the sensor does not need replacement. (H-2, H-6)	ST.CC2: Service technician must not replace the sensor unless the sensor needs to be replaced.
ST.UCA2b2: Service technician damages the sensor or other components while replacing the sensor. (H-4, H-5)	ST.CC3: Service technician must not damage the sensor or other components while replacing the sensor.
ST.UCA1c2: Service technician replaces the sensor after spending more than <X> minutes troubleshooting. (H-4)	ST.CC3: Service technician must identify sensor needs replacement in less than <X> minutes.
ST.UCA1d1: Service technician replaces the sensor but does not complete the repair. (example: doesn't plug in harness). (H-2, H-4)	ST.CC4: Service technician must complete the repair and verify repair.