Leibniz Online, Nr. 49 (2023)
Zeitschrift der Leibniz-Sozietät der Wissenschaften zu Berlin e. V.
ISSN 1863-3285 • DOI: 10.53201/LEIBNIZONLINE49

Safety and the Human-Machine Interface: The Importance of Cybernetic and Orgware Analysis in Safety Regulation

Vincent M. Brannigan
Clark School of Engineering, University of Maryland

Veröffentlicht: 1. Juni 2023

Abstract
The social control of technology is embodied in regulations of various types. To be effective, these regulations rely on feedback loops and, therefore, describe cybernetic systems. However, these systems can range from purely automatic systems to entirely human systems and are constantly evolving. Many technologies rely on a nested set of such systems that transfer information from one to another. By effectively classifying the systems using a combination of cybernetic and orgware characteristics, it is possible to properly analyze the regulatory effectiveness of the systems. Examples ranging from the sinking of the Titanic to the crash of a Boeing 737 MAX are used to illustrate the topic of the article.

Resümee
Die soziale Kontrolle der Technik ist in verschiedenen Arten von Vorschriften verankert. Um wirksam zu sein, sind diese Regelungen auf Rückkopplungsschleifen angewiesen und beschreiben daher kybernetische Systeme. Diese Systeme können jedoch von rein automatischen Systemen bis hin zu vollständig vom Menschen gesteuerten Systemen reichen und entwickeln sich ständig weiter. Viele Technologien beruhen auf einer Verschachtelung von kybernetischen Systemen, die Informationen von einem zum anderen übertragen. Durch eine effektive Klassifizierung der Systeme anhand einer Kombination aus kybernetischen und Orgware-Merkmalen ist es möglich, die regulatorische Wirksamkeit der Systeme angemessen zu analysieren. An Beispielen, die vom Untergang der Titanic bis zum Absturz einer Boeing 737 MAX reichen, wird das Thema des Beitrags anschaulich dargestellt.

Keywords/Schlüsselwörter
Cybernetics, orgware, safety regulation, technical innovation, social control
Kybernetik, Orgware, Sicherheitsvorschriften, technische Innovation, soziale Kontrolle

1 Cybernetics

Cybernetics comes from the concept and Greek name for a helmsman steering a ship (Greek κυβερνήτης or *steersman,* cf. Wikipedia 2023). The helmsman steers the ship based on a ***goal*** and a **feedback loop.** Feedback loops are a simple concept. The operator monitors a situation, compares it to a goal and changes the action based on the comparison. A cybernetic loop is schematically shown in Figure 1.

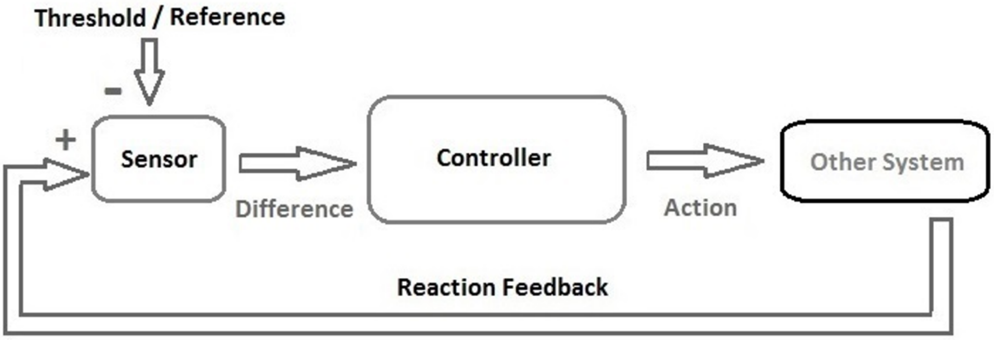


Fig.: Illustration of a cybernetic loop.

There are a variety of different ways of characterizing the feedback loop control system. This paper is focused on the role of feedback loops in safety regulation of technological products. Safety regulation is fundamentally the control of technological situations to achieve a social goal of reducing life or property loss. Regulation is an interface between law and technology to achieve public policy. Public policy may allow a certain level of risk or injury or hazard but that decision is beyond the scope of this paper. The purpose of regulation is to carry out the public policy.

Historically technical regulation dealt with technological objects that were relatively "static". Safety valves, boilers, railroad couplers, bridges, and so forth could be examined, certified and sent on their way. Occasional inspections were sufficient to confirm that the object was unchanged. However, in the more modern era technical regulation has moved from simple objects to complex systems. Consider the difference between a ship having a certain number of approved lifeboats and a requirement that the lifeboats be functioning as an effective rescue system. Having a system function correctly is far more complex than just an assembly of objects especially when the system depends on substantial human participation. Regulation of dynamic systems is therefore far more complex and the time scales for action are often shorter.

1.1 Cybernetic Regulatory Analysis

Regulatory analysis is designed to inform society as to whether a given regulatory system "works". Cybernetic Regulatory Analysis (CRA) is fundamentally the study of feedback loops critical to the regulatory process. Cybernetic analysis does not deal only with machines. Cybernetics can involve a purely human feedback loop. For example, in the ancient Code of Hammurabi:

> If a builder builds a house for someone, and does not construct it properly, and the house which he built falls in and kills its owner, the that builder shall be put to death. (Avalon Project Yale)

From a regulatory perspective this feedback clearly keeps the builder from building additional defective houses. Conceptually it is not different from revoking a professional license.

A cybernetic system is, therefore, one that is based on functioning feedback loops whether human or machine without regard to automation. CRA is examination of that system to determine if it meets social safety goals. CRA allows us to describe whether the feedback loop in the cybernetic system is functioning correctly in accomplishing the social goals. A distinguishing characteristic of CRA is that it can routinely expose inadequacies in the system BEFORE a disaster occurs.

1.2 Cybernetic Systems

There are a wide variety of types of cybernetic systems. Many cybernetic systems were originally created within or working directly with machines. *Cybernetic machine systems* can be described as a mechanized feedback loop system which controls the machine. One simple example is the traditional governor on a steam engine. In such a very simple system the cybernetic machine system works automatically to control the speed of the engine. Other cybernetic systems involve humans in various roles, from substituting for a machine function, to exercising operational discretion and finally to planning and design of the system. The result is that the is a range of cybernetic systems from pure machine to pure human.

1.2.1 Cybernetic System Functions

All cybernetic systems whether machine human or mixed have a series of specified functions (Figure 2). For this paper they are:

- *Goal setter*: describes what the system is trying to accomplish; it also functions as the system monitor
- *Sensor*: detects what the system is doing
- *Comparator*: compares the system functioning to the goal and determines deviation
- *Actuator*: adjusts the system to reduce the deviation from the desired goal

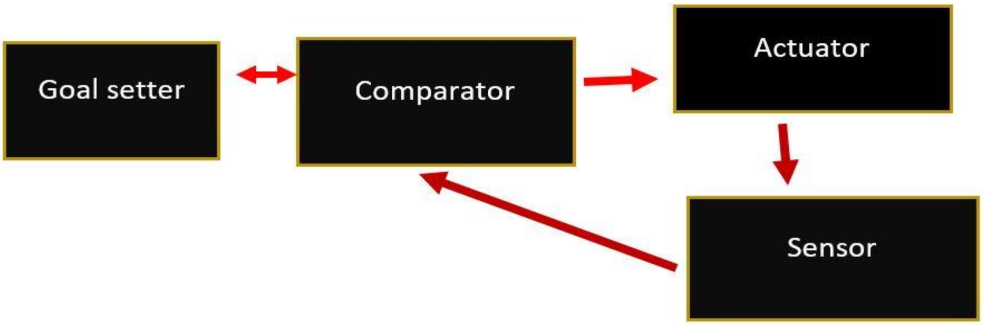


Fig 2: Relationship of the cybernetic systems functions.

These various functions can be seen in the traditional speed governor on a steam engine (Figure 3).

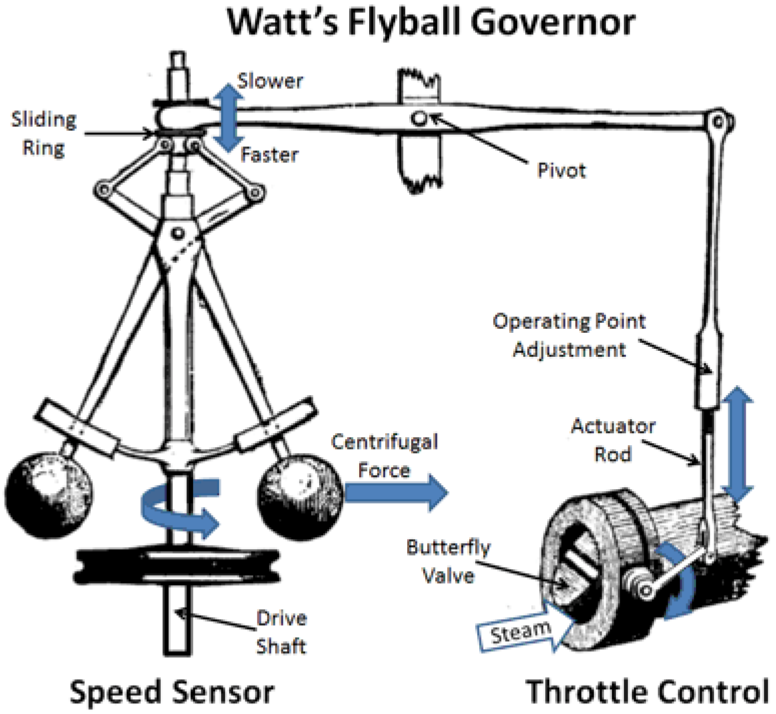


Fig. 3: Watt's flyball governor with the elements speed sensor and throttle control.

In this system as the drive shaft speeds up the balls swing apart and the linkage reduces the steam going through the pipe. As it slows down the reverse happens. The speed can be set within a very narrow range. This is a simple system and has existed for hundreds of years. It is a "static system" for the most part. Once set and maintained it will keep the engine running at the same speed.

1.2.2 Complex System

However most modern systems are far more complex. Even the namesake *cybernetic* system involving the helmsman on a ship is not a simple feedback loop dealing with one task. The helmsman of a sailing ship has multiple simultaneous tasks and goals:

1. Keep the ship safe, e.g., steering in accordance with the wind and waves and avoiding rocks or other ships
2. Keep in the ship on the desired compass heading (direction of the bow of the ship in a straight line)
3. Keeping the ship on the correct "course" to the objective (total movement of the ship to the objective). Compass heading and course are clearly separate tasks since a ship often has to change heading constantly to "make good" a base course
4. Keep the ship moving (sailing ship, e.g., sailing ships cannot sail directly into the wind)

These tasks and goals obviously interact. Because the wind is not constant both sails and rudder must be adjusted as wind changes to keep the compass heading constant. The compass heading must be adjusted continuously for the course. These actions may conflict and the conflict has to be resolved.

In this helmsman example the multiple feedback loops all return information to the same comparator. Each feedback loop can be a sensor for another feedback loop since the same decision maker is involved. So, from the beginning the choice of the term "cybernetic" required understanding that cybernetic functionality can be extremely complex and dynamic and can involve complex interactions between human and machine. Publicly regulating that functionality is even more complex than operating the system.

2 Regulatory Effectiveness Analysis (REA)

In general, the analysis of safety regulation requires a formal structure to conceptualize the achievement of social goals. One way of describing the structure is *Regulatory Effectiveness Analysis* (REA) (see Branigan 2007).

REA is a method for describing the compliance of a proposed technological system with an existing or proposed regulatory program. REA is designed to describe separately and together the three key components of a technical regulatory system.

- *Public policies*: Public policy is a narrative statement of the *goals* to be achieved by the regulatory program. Typical goals are acceptable safety, economic efficiency and distributional equity.
- *Legal structures:* Regulation requires a mechanism to enforce the social will on individuals or firms who would not otherwise comply. Legal structures are the formal requirements imposed by the society. They are described here in conceptual terms rather than specific laws or institutions since the concepts are multi-national. They must contain all necessary elements.
- *Technical tools:* Every technology has a distinct and often limited set of technical tools available for regulation. Tools include mathematical models, test methods, measurement techniques, “inspectability”, etc. They must be available and produce the needed results.

All three of these components must be properly designed to achieve a working regulatory system.

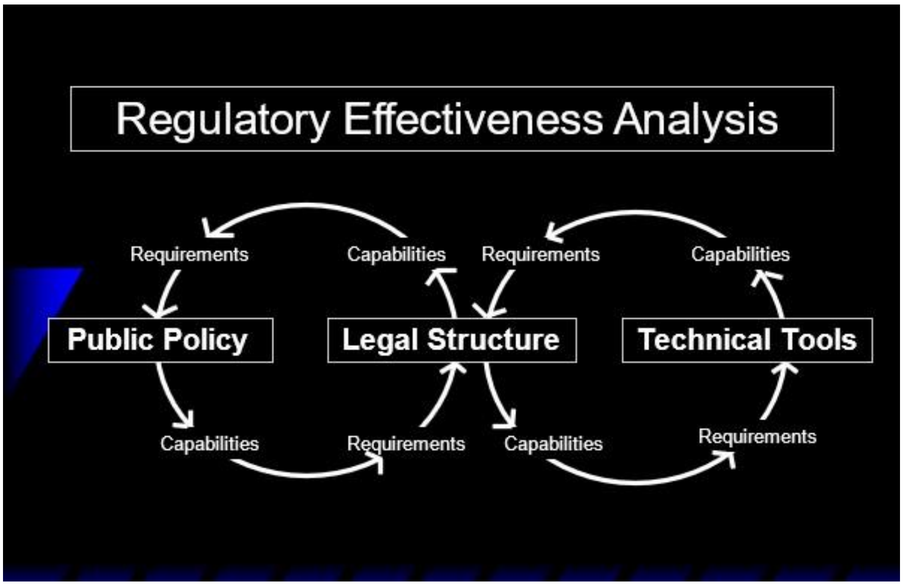
Public policies must be coherent.

The components also interact critically. Public policy, legal structures and technical tools have interlocking sets of requirements and capabilities.

Requirements are the preconditions which must be satisfied by other components before a given component can function.

Capabilities reflect the ability of a component to satisfy a requirement of another component.

For example, the legal structure may impose a responsibility on the *owner* of a building. It is often a *requirement* of such a structure that *ownership* is easily determined. A ship’s paper is a technical tool used to establish ownership. “Flags” have traditionally been used to describe the asserted nationality of a ship. The components can be integrated into a diagram (Figure 4):


Regulatory Effectiveness Analysis

Public Policy

Legal Structure

Technical Tools

Fig. 4: Diagram with the interaction of the components of the Regulatory Effectiveness Analysis.

2.1 Discontinuity

Public policy, legal structures and technical tools must be matched to one another (through requirements and capabilities) to produce a functioning regulatory program. If a component is ill defined or there is no match between policy goals, structure and tools, a discontinuity exists. A discontinuity routinely results in a failed regulatory system and potentially a disaster.

It is unfortunately also common to establish a regulatory program based on vague policy goals and a limited legal structure. This can result in critical public policy decisions being buried in the technical regulatory structure. The discontinuity may only become obvious after a disaster.

As an example, in the Mont Blanc Tunnel fire, the technical tool used for fire safety regulation related to the "ignitability" of a cargo. However, the hazard of a heavy goods vehicle in a tunnel fire is also related to the effective heat of combustion of the cargo. At Mont Blanc Tunnel, vegetable oil was allowed in the tunnel but kerosene was banned even though they have virtually identical heats of combustion. The result was a disaster. Avoiding such discontinuities is a major focus of technical regulation.

2.2 Dynamic Technical Regulation

The Mont Blanc Tunnel fire safety was essentially a static system. Applying a regulatory framework to modern dynamic systems requires far more sophisticated technical tools. Most users are familiar with dynamic cybernetic systems in daily life. Users monitor the battery in a mobile phone to make sure we can make a call. Users monitor the "bars" to make sure we have reception. In cybernetic regulation we have a public agency performing the same function. Dynamic environments require continuous regulation similar to the dynamic regulation used for regulated professionals such as physicians, lawyers and engineers and to certain hazardous activities that demand continuous regulation such as air traffic control. All of these involve more or less continuous monitoring of activities combined with a corrective feedback loop.

One of the simplest and most universal dynamic regulations based on feedback loops are driving licenses. Driving license holders are monitored regularly by a complex feedback loop of police, machines, courts and administrative agencies. Based on feedback driving licenses may be removed or restricted. This is a simple version of the more complex regulation of professionals and their feedback loops.

The distinguishing characteristic of these professional and high hazard regulations is that they rely even heavily on "feedback loops" and are therefore cybernetic regulations.

3 Cybernetic Regulatory Analysis

The critical element is the interaction between the legal structure and the technical tools in effectuating the public policy. While the driver's license example uses direct government cybernetic regulation, in complex technical systems it is more common for regulators to require the regulated organization to have a meaningful internal regulatory system since in these environments the feedback loops have to operate in "real time" to avoid disaster. The regulatory system goal is to have the regulated entity to operate a fast-acting self-regulated cybernetic structure with supervision by public authorities. Such systems rely heavily on appropriately structured multi-level transparent feedback loops.

Cybernetic Regulatory Analysis is the evaluation of regulated systems that normally have multiple types of feedback loops. Cybernetic Regulatory Analysis can be used on many types of "systems" including machine, integrated or human that has or should have feedback loops. The purpose of the CRA is to determine if the system is successful in meeting the articulated policy goals. The lack of an effective feedback loop is a cybernetic failure. Specifically cybernetic controls themselves are a technical tool and need to meet the interlocking requirements and capabilities of the legal structure.

3.1 Cybernetics: Deconstructing the Helmsman's Tasks

Cybernetic regulatory analysis is most useful on systems that are complex and dynamic. Driving an automobile to a destination involves numerous layers of cybernetic systems from automatic systems controlling the engine to humans deciding the goal of a journey, or even deciding what type of automobile to acquire. These are all separate but interacting systems. As noted above the "helmsman" of a ship has a whole series of tasks which map onto cybernetic functions. These include:

- Controlling the rudder or sails (activator function)
- Observing the compass heading (sensor function)
- Determining the appropriate course to the goal (comparator function)
- Reacting to dangers and changes (sensor, comparator and activator)

In larger ships, these tasks were so complex that the job was routinely subdivided and a series of interacting cybernetic systems was created. For example, the rudder control system itself was first mechanized and then automated (creating a machine system). The person controlling the rudder was now routinely called a quartermaster. The quartermaster no longer determined the compass heading or course but followed specific orders stated as a compass heading. In this case, the human is part of a human machine interface. This is an actuator function and requires reaction but not discretion or decision making.

A navigator now determines the position of the ship and sequential compass headings for the quartermaster that would take the ship on the desired course to reach the final goal. This is a comparator function.

A commander determined final goals for the navigator and gives safety orders directly to the quartermaster. This is goal setting.

In steamships, the control of engine speed and reversal passed to an engineer who was part of a human-in-machine system.

The output of this "helmsman disaggregation" process is a complex multi person cybernetic system. Regulating such a system requires careful analysis.

Traditional machine oriented cybernetic systems routinely had two separate levels. Automated systems automatically react to inputs with outputs, e.g., Watt's governor and its progeny. Auto pilots for aircraft represent such a system. They are entirely automatic.

Human-in-machine systems exist where we expect the human to react predictably and reliably as part of the human-machine coupling. In the ship example, the quartermaster is the human part of the human-in-machine system. Human-in-machine systems are sometimes in a transition stage to full automated systems, e.g., celestial navigation to GPS. A navigator is acting with a sextant, a chart, tables and a chronometer in a human-in-machine system. The engineer is controlling the engine. In many cases, the human is performing routine tasks that could be automated but is also needed for emergencies beyond the automated system capacity. The inner cybernetic fully-automated device is a part of the outer human-in-machine-system.

"Driverless" cars may represent such a transition from human-in-machine to full automation. In such cases, the human is a kind of safety system for the complex automated systems. These two types of systems are the traditional domain of cybernetics.

3.2 Orgware

But since feedback loops are also present in purely human systems cybernetic analysis can be extended to such systems, especially systems interacting with or controlling machines. To understand these far more complex "human cybernetic systems" it helps to use the concept of orgware to describe the human development and control of the traditional cybernetic systems. Orgware was first proposed by Dobrov (see Dobrov 1979).

Since it is a control system, orgware routinely has or should have feedback loops. Cybernetic analysis can therefore be applied to orgware. This paper proposes that orgware can also be thought of as operating on two distinct levels that "wrap around" the two traditional cybernetic domains.

To use the ship example the commander, the lookout and the dead reckoning navigator are all part of an orgware system that operates the system. This layer "wraps around" the human-in-machine level and can be described as the operative level. The operative level is designed to use the system to carry out the desired result.

The outermost level can be described as the planning level The planning level determines the basic structure and rules and goals of the entire operating system. The different levels can be incorporated together in a single diagram (Figure 5).

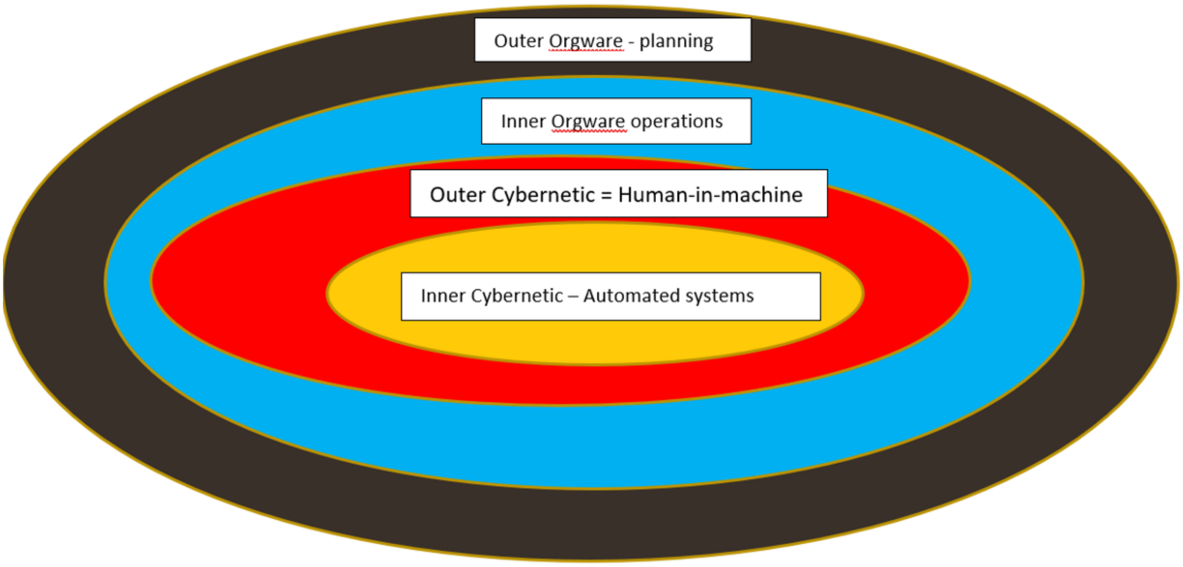

Outer Orgware - planning
Inner Orgware operations
Outer Cybernetic = Human-in-machine
Inner Cybernetic – Automated systems

Fig. 5: The levels of the orgware operating system.

3.3 Combining Orgware and Traditional Cybernetics System Thinking

- All activities that shape and develop the system are *outer orgware.*
- All activities that operate the system and can be part of it are *inner orgware.*
- All human-in-machine activities are *outer cybernetic.*
- All automated systems are *inner cybernetic.*

Obviously, there can be multiple feedback loops within each ring. Some are inputs to another loop in the same ring and others are inputs to the next ring out.

Feedback loops: Feedback loops are characteristic of both the traditional cybernetic and orgware systems These systems also interact with one another in several ways. For example, a human might be part of a human machine coupling some of the time and part of operative orgware other times, e.g., dead reckoning versus celestial navigation. Automated systems can both signal humans to take actions and record and transmit information back to the planning level. Radar can be a sensor.

While feedback loops are characteristic of traditional cybernetic systems, orgware systems also need effective feedback loops and failure to provide an adequate feedback loop can lead to a disaster. To avoid disasters, we must have regulatory controls that ensure that both planning and operational levels have suitable feedback loops. One example of an orgware cybernetic loop regulation is the US Food and Drug administration (FDA) regulation of medical device complaint file.

§ 820.198 Complaint files (see FDA 1996-2013):

> (a) Each manufacturer shall maintain complaint files. Each manufacturer shall establish and maintain procedures for receiving, reviewing, and evaluating complaints by a formally designated unit. …
>
> (b) Each manufacturer shall review and evaluate all complaints to determine whether an investigation is necessary. When no investigation is made, the manufacturer shall maintain a record that includes the reason no investigation was made and the name of the individual responsible for the decision not to investigate.

> (c) Any complaint involving the possible failure of a device, labeling, or packaging to meet any of its specifications shall be reviewed, evaluated, and investigated, unless such investigation has already been performed for a similar complaint and another investigation is not necessary.
> (d) Any complaint that represents an event which must be reported to FDA under part 803 of this chapter shall be promptly reviewed, evaluated, and investigated by a designated individual(s) and shall be maintained in a separate portion of the complaint files or otherwise clearly identified.

These FDA required complaint files are a critical feedback loop in both planning and operational activities. From a regulatory perspective it is fairly easy to make sure device complaints are logged and investigated and a sample can be examined in greater detail. Many physician users file complaints with both the FDA and the manufacturer. There is no greater deterrent to a firm than realizing the FDA inspector can ask for a complaint by date and sender and the consequences if the firm cannot produce it.

4 Defective Feedback Loops

Defective feedback loops fail to give suitable inputs to decision makers. The most important characteristic of defective feedback loops for safety regulation is that they can be routinely discovered and analyzed prior to the disaster. Defective feedback loops can also corrected prior to adverse incidents. This is the core of Cybernetic Regulatory Analysis. Recall the four elements of a feed-back loop are

- Goal setter
- Sensor
- Activator
- Comparator

A few minor case examples show the specific issues. It is important to remember that the concept of the cybernetic feedback loop operates simultaneously at all levels The output at each level is an input to the levels above.

4.1 Defective Feedback Loop – ICE Crash Eschede

The fatal Eschede train crash occurred in Germany in 1998. While there are many other issues involved, the most important feedback loop was the operative loop controlling the actions of the conductor who was aware of severe vibrations but did not stop the train: Upon finding the conductor (Passenger Dittmann was informed that it was mandatory to evaluate the possible damage before triggering an emergency stop. (Schroeder 2020)

This delay allowed the crash to unfold disastrously. So, the human sensor detected vibrations but the human activator was delayed to find a cause for the alert. The defective assumption was that waiting to find the cause does not make it worse. This error was made at the planning level. That error created the "human error" at the operational level.

4.2 Defective Feedback Loop Lathen Maglev Crash

Two vehicles crash into one another at high speed on a single closed track. The Lathan maglev crash occurred because the planning level put critical safety decisions at the operational level rather than automate the safety system. That failure would have been obvious in a trivial analysis of the feedback loop. Defective feedback loops of this type are routinely and prematurely described as human error rather than doing a proper analysis of the feedback loop. In a cybernetic regulatory analysis, the Lathan crash was defective design of the system not human error.

4.3 Boeing 737 MAX – Cybernetic Machine

The 737 MAX contains an autonomous "intelligent" aircraft control system. The computer-controlled stability system is itself an inner cybernetic device subject only to partial human control. The failure to organize and understand the limited human control arguably killed 346 people in two completely preventable crashes.

The goal of the designers of the 737 MAX was simple: to meet competition from the Airbus 320. They wanted to put bigger more economical engines on the 737. The problem was the bigger engines would not fit under the wing so the answer was to put them further forward and higher. As the 737MAX was being designed and tested it was clear it exhibited dynamic instability under some circumstances.

In an emergency pilots routinely add power to gain altitude and control. But when pilots added power to the 737 MAX at high "angles of attack" the plane could go into a catastrophic stall. The 737 MAX's more powerful engines were far enough forward and higher so that the application of power would cause the airplane nose to "pitch up" and endanger the control of the aircraft by putting it into aerodynamic stall.

Angle of attack: The angle of attack is critical to flight. It is the angular difference between the forward motion of the aircraft and a straight line through the aircraft. Excessive angle of attack leads to "aerodynamic stall". An aircraft in stall is in immediate danger of crashing. Preventing stall and recovering from stall are absolutely fundamental design criteria and the most critical part of pilot training.

To solve the dynamic instability problem Boeing produced a fully automated system called the Maneuvering Characteristics Augmentation System (MCAS). The MCAS was designed to feedback information from the angle of attack sensor directly to the aircraft controls and prevent aerodynamic stall by pushing the nose down using the horizontal stabilizer on the tail of the aircraft. MCAS was a fully automatic system effectively unknown to the pilots or airlines.

The MCAS used input from the angle of attack sensors. Commercial transports carry a pair of electromechanical "angle of attack" sensors on the outside of the aircraft. Feedback from these sensors is often critical to control of the aircraft. But these sensors are essentially "weathervanes" on the outside of the aircraft. They are fragile and vulnerable to damage. They are duplicated as a safety measure. The MCAS was designed to use information from the angle of attack sensor to automatically detect an "nose up" and manipulate the aircraft's horizontal stabilizer to push it down

However, the MCAS system was tied to a single angle of attack sensor instead of using and comparing both sensors and had no system for dealing with defective information from that sensor. This planning decision created a "disaster waiting to happen". Very simply if the angle of attack sensor is providing incorrect information the MCAS can cause the plane to crash by pushing the nose down. Boeing also did not tell the pilots the MCAS system existed. Or what to do if it failed. This was a planning decision to make the aircraft more saleable by not requiring MCAS training. A defective sensor in the Lion air flight repeatedly pushed the aircraft's nose down until the pilots lost control and the aircraft crashed. After the Lion air crash, Boeing said pilots to shut off the MCAS system in the case of emergency.

The second emergency was on Ethiopian Airlines. But when the pilots followed the Boeing instructions and shut off the MCAS they also lost the power control over the horizontal stabilizer. There was no fundamental reason for this interconnection. It was a planning decision. When the pilots shut the power off, they could not control the airplane without the power assist. When the pilots turned the power back on the MCAS continued to drive the nose down and the plane eventually crashed and 156 people were killed.

4.3.1 Boeing 737 MAX – Cybernetic Analysis and Orgware Planning Level

Moving the engines forward and their larger size and power created the instability. The computer software system (MCAS) that was driving control systems was designed and installed to counteract the instability. By not drawing attention to the instability or MCAS's role Boeing avoided having to recertify the aircraft and retrain pilots. MCAS had a single point of failure. If the angle of attack sensor failed the system could crash the plane. No precautions were included for the known risk of a defective sensor. In case of a runaway stabilizer, the only instruction was cutting power which also removed the power assist for the stabilizer.

In the case of the 737Max it would appear that Dobrov's orgware was the key location for cybernetic failure. There was inadequate risk analysis. The Boeing orgware system did not require that the direct operators have an adequate understanding of the computer software.

It should be especially emphasized that every aspect of this failure was knowable at the planning level!

4.4 RMS Titanic

RMS Titanic was:

- The largest and most modern ship in the world
- Built by an experienced UK builder without limit on price
- Operated by an extremely experienced shipping firm
- Manned by the most experienced sea officers
- Inspected and regulated by the Board of Trade of the most experienced sea faring nation in the world.

So, what could go wrong?

4.4.1 Ship Safety Orgware – Planning and Operative

Safety Planning – Captain Smith had specific and direct instructions not to risk the ship to save time:

- the vital importance of exercising the utmost caution in navigation,
- safety outweighing every other consideration,
- over confidence should be especially guarded against a cautious, prudent and ever watchful system of navigation which shall lose time or suffer any other temporary inconvenience rather than incur the slightest risk which can be avoided. (TIP 2012)

However, there is no evidence that anyone ever checked that Captain Smith was actually following these instructions. There was no feedback loop on his navigational safety.

4.4.2 Operational Safety

On the night of the collision Titanic turned westerly at full speed at night directly into the ice field in poor ice visibility conditions (flat calm seas) and no moon. Captain Smith could have run south of the icefield on a safe course as was done by SS Mount Temple. That would have been in accordance with his instructions. But Captain Smith had run through icefields at night before and never hit one. From this he believed that it could be done safely, rather than that he had merely been lucky. No one in the White Star Line seems to have taken notice of this risk taking. So, the planning/operational feedback loop was defective.

The risk of hitting an iceberg depends on ship handling and visibility. At 41.7 km/h, it appeared that Titanic could not stop or turn in its visual sighting distances for an iceberg in the North Atlantic at night. The calculated stopping distance fully loaded at 41.7 km/h is 1000 m plus "delay time" in sighting the iceberg and passing instructions to the engine room. Given a reasonable reaction time at 22.5 knots (41.7 km/h) Titanic had to be able to see an Iceberg more than 1400 meters ahead. The night of the collision there was no moon so the sky was pitch black, plus there were no waves to reveal icebergs and therefore it was the worst possible visibility. No binoculars or even goggles were issued to lookouts who were expected to carefully stare into a freezing cold wind.

Icebergs can be very big many times the size of the Titanic. Sailors can sometimes see icebergs above the horizon at night by the icebergs "occulting" stars. But when the iceberg is close enough to be "below the horizon" it is much harder to see. From the Titanic look out position the horizon was 10 miles (16 km) away. No one seems to have connected the requirements for stopping or turning to the lookout's ability to see an obstruction. It appears that the question was never asked, which is a clear orgware planning failure. The reason for the failure is almost certainly Titanic's massive size. With its sister the Olympic they are far and away the largest ships in the world. Feedback on avoiding icebergs from with smaller ships was irrelevant. The result was a tragic but entirely foreseeable disaster.

4.4.3 Cybernetic Regulatory Analysis

The core similarity between the Titanic and the 737 MAX cases is the introduction of a new technology into an existing technical regulatory system. The hardware in both cases was "inadequate" but not because of any novel or different technology. Instead, it could be explained that defective orgware allowed the propagation of risk due to easily described but major failures in orgware at all levels.

4.4.3.1 Multi Actor Problem

The Titanic also gives a fascinating example of perhaps the most complex cybernetic regulatory problem, the "multi actor problem". All the case examples given above deal with a single organizational actor. But some problems are multi actor cases.

4.4.3.2 Rescue at sea

The Titanic was specifically allowed a reduced outfit of lifeboats due to bulkheads and the availability of wireless telegraphy and accurate navigation. It was assumed that other ships would promptly come to the rescue of a ship in distress and that boats were a "transfer system" to other ships. In other words, Titanic did not need lifeboats for all since the captain could call for help. However, a cybernetic analysis of this planning decision would show its absurdity in 1912.

For the suggested rescue system to work the positions of ships at sea had to be coordinated. In particular all ships had to have wireless running 24/7 and both know their own position and regularly transmit it to other ships in rescue range. Wireless operators had to cooperate despite the known commercial rivalry of Marconi and Telefunken. Captains had to be prevented from going outside of rescue range of other ships. All of this is obvious in a cybernetic analysis but none of it was done.

4.4.3.3 Navigation

Navigation is knowing where the ship is and is going. In 1912, the ship position was both a human-in-machine system and an operative system. Ship's officers' fundamental and crucial responsibility was determining the position of the ship at sea. The ability to navigate a ship was the major focus of the Board of Trade licensing of the officers.

Using celestial navigation, the officers were essentially calculators, there was no "judgement" involved. In 1912 under the conditions at the time of the collision, each officer was capable of using celestial navigation to fix the ships position within a 1.5 km circle. Celestial navigation is an extremely complex combination of hardware and calculation. It requires a sextant, a chronometer, knowledge of the stars and considerable mathematical calculation. The celestial navigator is a "human-in-machine" in determining position. It requires no judgment only technical skill.

The second form of navigation in 1912 was "dead reckoning". Using the officer's knowledge of the ship, its speed and course, and recorded knowledge of currents, navigators at sea plot a course from the last known (celestial) position. Dead reckoning is operative. It is checked against celestial navigation which acts as a feedback loop. However, both of these are useless in an emergency unless the positions are properly recorded in a logbook or plotted in a chart. In the Titanic, no one kept continuous track of the position. From the UK Board of Trade inquiry (see TIP 1912):

- 15223. [Commissioner] How often when you are on watch do you mark the position of the ship on the chart? – [Officer Pitman] Only at noon.
- 15224. Do not you mark it again? - No, not when we are well at sea.
- 15225. You do not mark it when you go off watch for the purpose of letting the man who succeeds you see at once on the chart where the ship is? - No, only when we are making (approaching) the land.
- 15226. Do you do it when you get a stellar observation? - No, my Lord, unless we are making the land.

Titanic moved over 800 km per day but the navigator's accurate celestial position was charted only once per day. As a result, when Titanic hit the iceberg, they did not know exactly where they were. The critical 8 pm dead reckoning position was written on a "chit" of paper and left on the chart room table. When the ship struck the iceberg, they had to "work up" a position and did it wrong, several times. An incorrect position was sent to rescuers (off by 25 km).

No one required the ship to have a system for recording and knowing its position at all times. The captain, the White Star Line and the Board of Trade did not require it. They simply did not treat knowing the exact current position of the ship as a critical requirement. Titanic's navigation was a defective operational feedback loop. The failure to require plotting was a defect in planning. It must also be noted that not knowing their precise position also meant they could not effectively use the ice warnings from other ships with any reliability or call for help.

4.4.3.4 Marconi Radio System

Titanic had the best most modern wireless system afloat. However, the Marconi room had no direct communication with Titanic's bridge, which made the use of wireless information very difficult. This was the result of planning decisions, in particular "Contracting out". Marconi is a separate company that provided equipment and men running a telegraph business on board. There was no clear relationship between the Marconi operators and the captain in regard of navigation or safety. In the crew list the Marconi operators are listed in the stewards' department not the navigation department. Marconi was running a very lucrative business on board.

The operators received regular ice warnings via radio for example 9:40 pm, a message from the westbound SS Mesaba (Titanic was also westbound just behind Mesaba):

> From Mesaba to Titanic and all eastbound ships. Ice report in latitude 420N to 410 25'N, longitude 490W to 50030'W. Saw much heavy pack ice and great number large icebergs. Also field ice. Weather good, clear. TIP 2012

This message never made it to the bridge. The Marconi operators were too busy with commercial traffic. Captain Smith had set up no system to make sure he got ice warnings. 11 pm there was a message from the Californian: "We are stopped and surrounded by ice." Marconi operator Phillips retorted: "Shut up, shut up. You're jamming my signal. I'm busy. I'm working Cape Race." The Californian was only a few miles from Titanic. This message also never went to the bridge. (TIP 2012)

I conclude Titanic's radio warning system had defective feedback loops at both planning and operative levels. At the planning level nothing integrated the wireless into the ship's navigational safety. At the operative level, Smith did nothing to ensure that officers on duty would promptly get all the ice messages.

The multi actor problem of rescue at sea clearly requires sophisticated system thinking at the planning level of all the ships involved.

5 Cybernetic Regulatory Failures

These are just a small "smattering" of the vast number of regulatory failures that would have been disclosed by proper cybernetic regulatory analysis before the event. Other failures included:

- Concorde (inadequately disclosed need for a sterile runway before every take-off),
- Standseilbahn Kaprun (funicular railway was built to fire standards for an elevated gondola based on the fact it was a Seilbahn),
- Grenfell Towers (new cladding approved due to a demonstrably inadequate and out of date standard),
- American Airlines 457 (failure to inform pilots that use of rudder in flight could destroy airplane),
- Brandenburg airport. No deaths but billions in cost, but failure to have any orgware in place to integrate fire safety into construction planning,
- ATR 42 and 72 Auto pilot could encounter progressively dangerous condition without notification to pilot and then turn off leaving plane unflyable.

In these and many other cases adequate Cybernetic Regulatory Analysis would have disclosed the failure path prior to the disaster.

6 CONCLUSION

Cybernetic and orgware analysis provide powerful tools for analyzing complex safety regulatory problems involving modern technology. Safety must be analyzed as an integrated whole in which design production and operational decisions are included in the regulatory process. This paper proposes a simple analytical approach that integrates the cybernetic and orgware concepts and allows placement of complex systems into an integrated approach

- All activities that shape and develop the system are outer orgware.
- All activities that operate the system and can be part of it are inner orgware.
- All human-in-machine activities are outer cybernetic.
- All automated systems are inner cybernetic.

Feedback loops exist both within each layer and in the process of passing information between layers. The sender and receiver of information must be coordinated at all steps in the process. By examining all critical feedback loops it is possible to detect ***discontinuities*** prior to a disaster. Since the different levels are routinely created by different design and organizational teams an integrated approach will tend to break down "silo" thinking on the same level, unreasonable reliance on supposed actions on a different level, and emphasize the importance of top-level planning in anticipating potential disasters.

Bibliography

Avalon project Yale https://avalon.law.yale.edu/ancient/hamframe.asp

Brannigan, Vincent M. (2007): *The Regulatory Use of System Safety Analysis: A Regulatory Effectiveness Analysis*. 9th Bieleschweig Workshop, http://www.rvs.uni-bielefeld.de/Bieleschweig/ ninth/BranniganB9Slides.pdf (last access 10.4.2023).

Dobrov, Gennady M. (1979): "The strategy for organized technology in the light of hard-, soft-, and org-ware interaction". *Long Range Planning* 12 (4) 79-90. Available at https://www.sciencedirect.com/science/article/abs/pii/0024630179901249

Failure to Act (2023): *The Titanic and the Ice Warnings*. http://www.paullee.com/ titanic/icewarnings.php (last access: 10.4.2023).

FDA – US Food and Drug Administration, *Code of Federal Regulations* (1996, 2004, 2006, 2013): [61 FR 52654, Oct. 7, 1996, as amended at 69 FR 11313, Mar. 10, 2004; 71 FR 16228, Mar. 31, 2006; 78 FR 58822, Sept. 24, 2013].

Schroeder M The Cost of Comfort: The 1998 Eschede Train Derailment 2020 https://mx-schroeder.medium.com/the-cost-of-comfort-the-1998-eschede-train-derailment-4809dde1c450

Titanic Inquiry Project – TIP (1912): *British Wreck Commissioner's Inquiry – Report on the Loss of the Titanic*. https://www.titanicinquiry.org/ BOTInq/BOTReport/botRep01.php (last access 10.4.2023).

Wikipedia (2023): https://en.wikipedia.org/wiki/*Cybernetics* (last access: 10.4.2023).

Additional literature related to the topic of this article:

Fuchs-Kittowski, Klaus (1991): *Systems Design. Design of Work and of Organization – The Paradox of Safety, the Orgware Concept, the Necessity for a New Culture in Information Systems and Software Development*. In: Peter Van den Besselaar, Andrew Clement, Perttu Järvinen (Eds.): *Information System, Work and Organization Design*. Amsterdam, New York: North-Holland Publishing Co.,. 83 – 97.

Fuchs-Kittowski, Klaus (2020): „Informationssystem, Arbeits- und Organisationsgestaltung in Produktion und Verkehr – das Orgwarekonzept, die Paradoxie der Sicherheit, des Wächters, der Beherrschung großer Datenmengen". In: Brödner, Peter / Fuchs-Kittowski, Klaus (Hrsg.): *Zukunft der Arbeit – Soziotechnische Gestaltung der Arbeitswelt im Zeichen von „Digitalisierung" und „Künstlicher Intelligenz"*, Abhandlungen der Leibniz- Sozietät der Wissenschaften, Band 67. Berlin: trafo Wissenschaftsverlag.

Acknowledgement and Thanks

This paper was presented at the plenum of the Leibniz Society of Sciences in Berlin on the occasion of the awarding of the Wiener Schmidt Prize for achievements in the field of cybernetics on 13th October 2022 to Klaus Fuchs-Kittowski. The author would like to note his gratitude for a 40-year collaboration with Klaus Fuchs-Kittowski who sparked his interest in orgware and cybernetics. The collaboration began due to Klaus Fuchs-Kittowksi's interest in Dr. Margaret Dayhoff's work. Margaret Dayhoff is known as the "Mother of Bioinformatics". She is also the mother of Dr. Ruth Dayhoff, a world pioneer in medical informatics and the wife of the author.

The following photograph was taken in Adelphi, Maryland, in November 1982. From left to right: Prof. Vincent M. Brannigan, Prof. Klaus Fuchs-Kittowski, Dr. Ruth Dayhoff, Prof. Steven Spivak, Prof. Margaret Dayhoff.

E-mail address of the author: firelaw@firelaw.us