Human Design Parameters for Safety of Products and Systems

Kenji Iino[1,*], and *Masayuki* Nakao[1]

[1]The University of Tokyo, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

Abstract. Designers spend much efforts in defining their products and systems, planning how they work during normal operation. Design assisting tools like Design Matrices in Axiomatic Design (AD) or Design Record Graphs (DRG) are available to the designer in search for ways to improve their work. Majority of accidents, however, take place during irregular operations like maintenance when interlocks are often bypassed and automatic processing are switched to manual. System safety is then in the hands of human operators. A number of past AD studies have addressed safety in products and systems, however, design parameters (DPs) have been physical parts or structures. This paper shows assignment of human actions, like, "reading the quantity display," "making judgement," or "pressing a control button," as DPs in axiomatic design. Such human DPs play important roles during maintenance, nevertheless, designers often leave out safety evaluation of their designs in this maintenance mode. When a human DP fails to meet its functional requirement (FR), the product often faces failure and the system often heads into an accident. Identifying human DPs in products or systems thus alerts maintenance phase workers about actions that are critical for safety. Most accidents take place with excessive dependence on human DP of memory.

1 Introduction

1.1 The Water Faucet Problem

Often used as the first example in teaching Axiomatic Design (AD), we are all familiar with the hot and cold water faucet problem [1]. The two functional requirements (FR) are to adjust FR1: the water temperature, and FR2: the water flow rate to ideal ranges.

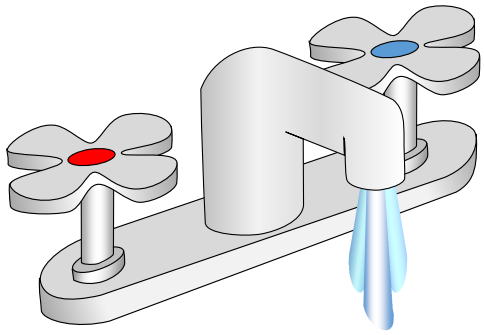

Fig. 1. Simple hot and cold water faucet

The design equation in this case shows a clear interference for the two design parameters, DP1: turning the hot water knob and DP2: turning the cold water knob. The design is coupled.

$$\begin{Bmatrix} \text{temperature} \\ \text{flow rate} \end{Bmatrix} = \begin{bmatrix} X & X \\ X & X \end{bmatrix} \begin{Bmatrix} \text{hot water knob} \\ \text{cold water knob} \end{Bmatrix} \quad (1)$$

Equation (1) shows the design equation of the system and Fig. 2, the Design Record Graph (DRG).

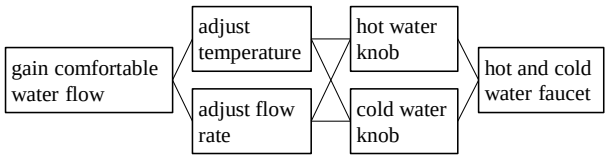

Fig. 2. DRG of the simple hot and cold water faucet

This problem is ideal for first teaching the concept of AD, however, a closer look reveals that the formulation has completely left out human factors. They are the operator sensing the water temperature with hands, the flow rate also with hands and possibly assisted with the water flow sound through the ears, making the judgement of which handle to turn in which direction by how much, and actually applying torque to the handles.

In this section, we will first show how the design equation changes with the inclusion of human interaction in reaching the desired FRs with the water faucet problem. We will then discuss a better design faucet and its problem when human factors come in play and yet another improvement common in Japan.

The second section discusses how designers often leave out human factors in their design. The problem is designers are concerned only about their designs in operation and not much thoughts are given to maintenance phases. Section 3 then explains a recent fatal industrial accident and applies AD analysis with human factor. Section 4 shows how our AD analysis

* Corresponding author: kiino@sydrose.com

with human factor can identify serious risks with designs, followed by our conclusions in Section 5.

1.2 The Water Faucet Problem with Human Factor

Fig. 2 shows the human interaction with the water faucet. The user has two active things to do; one is to adjust the hot water knob rotation, and the other is to adjust the cold water knob rotation. The user also has to sense the water flow rate and water temperature. In addition to sensing the flow rate with the feel of water falling on the hand, the user's eyes and ears receive visual and audible signals to help judging if the flow rate is ideal or not. The hand is the only practical receptor for the water temperature sensing.

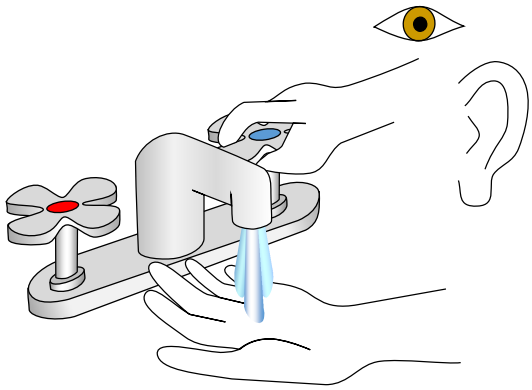

Fig. 3. Human adjusting hot and cold water faucet

Fig. 4 shows the DRG of this system. The user human and the water faucet system works together for obtaining a comfortable water flow. Equation (2) is the design equation.

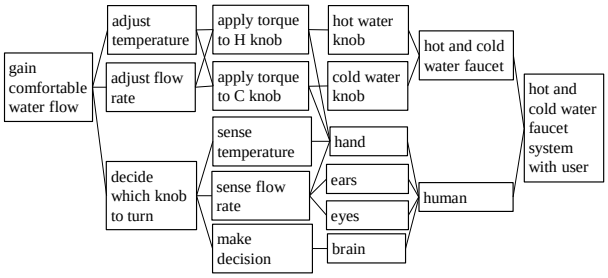

Fig. 4. DRG for human adjustment of hot and cold water faucet

$$\begin{Bmatrix} \text{apply torque to H knob} \\ \text{apply torque to C knob} \\ \text{sense temperature} \\ \text{sense flow rate} \\ \text{make decision} \end{Bmatrix} = \begin{bmatrix} X & 0 & X & 0 & 0 & 0 \\ 0 & X & X & 0 & 0 & 0 \\ 0 & 0 & X & 0 & 0 & 0 \\ 0 & 0 & X & X & X & 0 \\ 0 & 0 & 0 & 0 & 0 & X \end{bmatrix} \begin{Bmatrix} \text{hot water knob} \\ \text{cold water knob} \\ \text{hand} \\ \text{ears} \\ \text{eyes} \\ \text{brain} \end{Bmatrix} \quad (2)$$

The interference in Eq. (1) seems to be removed in Eq. (2), however, it is present in higher level of the DRG in Fig. 4, among the temperature and flow rate adjustment FRs and the torque application to H and C knobs FRs.

1.3 The Single Lever Solution

A solution known to have removed the interference with double knob design is the swivel lever design shown in Fig. 5. The lever has a spherical opening on its bottom that mates a spherical joint so the user can turn it up and down latitude-wise to change only the water flow rate and sideways longitude-wise to change only the water temperature. The design has a common name of single handle water faucet.

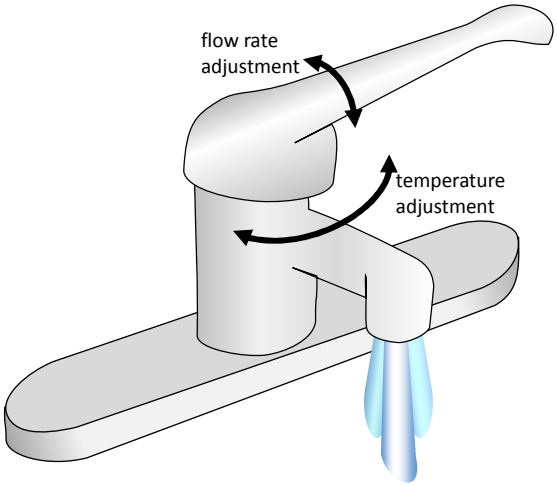

Fig. 5. Single handle solution for hot and cold water faucet

Figure 6 shows the DRG for the single handle design with human interaction. Note that the interference in Fig. 4 is now gone.

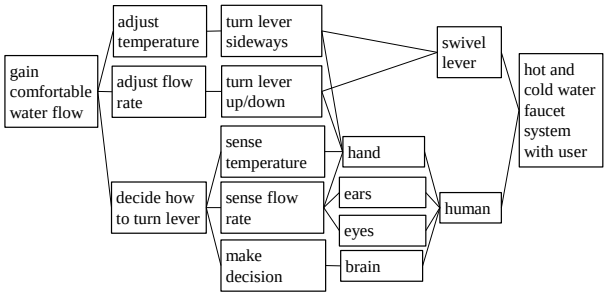

Fig. 6. DRG for swivel lever hot and cold water faucet

The single handle design, therefore, is theoretically a superior design, however, one of the authors, Iino often faced troubles using them. One reason is the 2 degrees of freedom (DOF) that the lever has in contrast to the 1 DOF for each of the hot or cold knob.

Increasing or decreasing the flow rate of hot or cold water with a knob is fairly clear with the simple right-hand rule; turn it counter-clockwise to increase the flow. With the swivel lever design, at an arbitrary point when the water is flowing, the user can rotate the lever into any direction to change the flow rate, temperature, or both at the same time. The operation, thus, burdens the brain in deciding how to turn the lever to change the conditions of the flowing water.

Another bothering factor is the non-standard directions for changing flow conditions with single lever water faucets. Probably in the US, the latitude-wise up

and down convention is; turn it up to increase the flow and down to decrease it. It is reasonable because when the seating of the spherical joint wears, gravity on the lever will tend to lower the lever, i.e., the direction of shutting the water flow off.

In Japan, however, many of the early designs worked the other way, i.e., to lift the lever to shut the water off. Unaware of this difference, Iino often had the problem of pushing the lever down, thinking that was the direction to shut the water off, and getting a gush of water in the wash basin and a splash of water on his pants.

The reason for this failure is the brain making a wrong decision. Fig. 6 shows this factor in the DRG by drawing human factors in it. A brain makes its decision based on logic, however, oftentimes, quick decisions are reached based on experience and habits.

1.4 Independent Control Solution

Figure 7 shows a solution often seen in public baths at hot spring resorts in Japan. It has an independent knob for water temperature control and a separate one for switching the flow to go to the showerhead or faucet and moving the mark further away from the neutral position increases the flow rate.

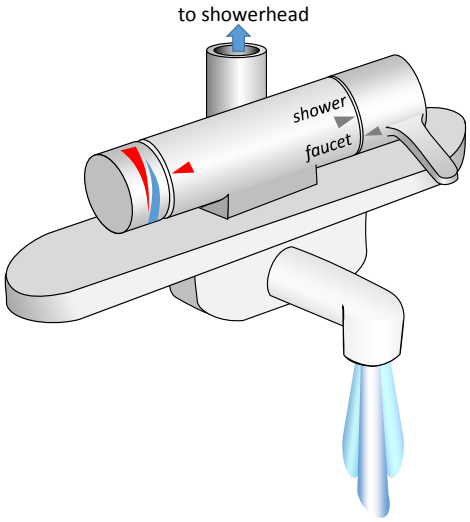

Fig. 7. Independently controlled shower/faucet

Reference [1] actually hints this solution as the first uncoupled solution to the coupled double knob design. The DRG (Fig. 8) for this design is clean without interference.

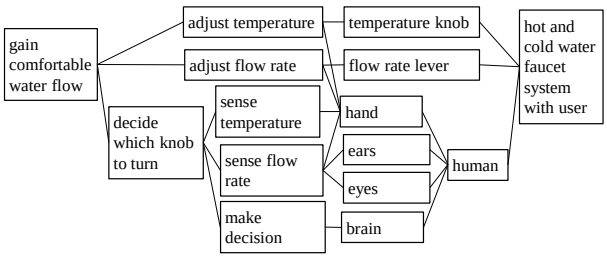

Fig. 8. DRG for independently controlled shower/faucet

2 Human Factor Evaluation

2.1. Designers Forgetful of Human Factor

We earlier pointed out that designers often leave out reliance on human operation from their design concepts [2]. Let's take a simple example of a flashlight to revisit this claim. Figure 9 shows parts of our flashlight to analyse and Fig. 10, a typical DRG of the flashlight by a designer when asked to draw a function-structure diagram (DRG) for it.

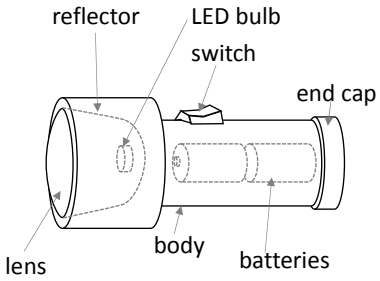

Fig. 9. Flashlight and its parts

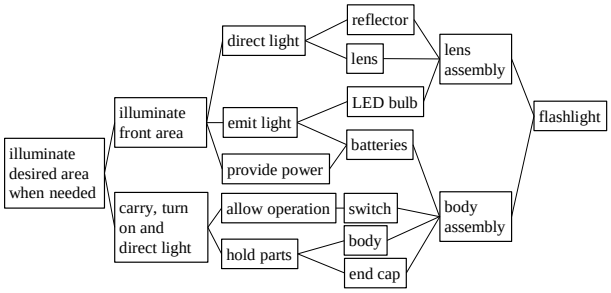

Fig. 10. Flashlight and its parts

Note in Fig. 10 that it is so easy to forget that the user has to turn the switch ON and direct the flashlight in the direction the user wants to illuminate. The user has to know how to push the switch to turn the light on and to move the arm and hand carrying the flashlight so the illuminated area matches the desired area.

2.2 Human Factor during Maintenance

Even simple products like a flashlight go out of order and we have to fix them unless we want to dispose it and go through the trouble of getting a new one.

A common failure of a flashlight is its batteries losing power and failure of the lightbulb. The lightbulb failure is now rare with LEDs, however, they were common with incandescent lightbulbs up until just a few years ago.

Now the user has a number of tasks to perform:

(1) Find and purchase the right replacement part,
(2) Open the end cap or lens assembly,
(3) Remove the failed part,
(4) Place the new part in place,
(5) Close the assembly back to the original state,

and in addition for protecting the global environment, we now have to know where to dispose the old batteries instead of tossing them into the garbage bin.

Figure 11 added human factors for the common battery replacement operation. Note that body parts, eyes, hands, and the brain are involved in every step.

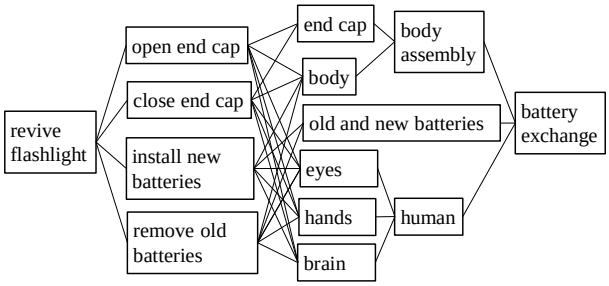

Fig. 11. Battery exchange operation of a flashlight

Although rare, a common failure of the battery exchange operation was to insert the batteries in the wrong direction, i.e., to reverse the positive and negative poles of the batteries. Surprisingly, the mistake could go unnoticed for some incandescent models, however, not with flashlights using LED lightbulbs.

To help the user insert batteries in the right orientation, many tools that require battery exchange have battery symbols printed inside the battery sockets so the users will not reverse the orientation. Mistakes that some people make come from the brain making the wrong decisions about orientation of batteries.

3 A Fatal Accident Case

3.1 Ethylene Plant Gas Quenching Line

On December 21, 2007, a fire broke out at Ethylene Plant 2 in Kashima Plant of Mitsubishi Chemical Corporation in Ibaraki Prefecture. Four employees of a contractor company lost their lives with this accident.

The accident took place after the decoking process of a furnace was finished. The furnace was a thermal decomposition furnace for ethylene production and refinement from crude gasoline, kerosene, and other material. Decoking removes coke (carbon residue) from the processing tubes using high-pressure water jet. During normal thermal decomposition, the furnace discharges exhaust gas for reprocessing. The gas discharge line has a quencher box after it leaves the furnace. Figure 12 shows a simplified outline of the furnace, gas discharge line, and its quencher.

Figure 13 is the quenching oil line configuration during normal operation. A ring-shaped spacer is in place. Figure 14 shows the DRG elements for this configuration. This is probably how far a plant designer will take the design concept. The design matrix for the elements in Fig. 14 will show a clean uncoupled design.

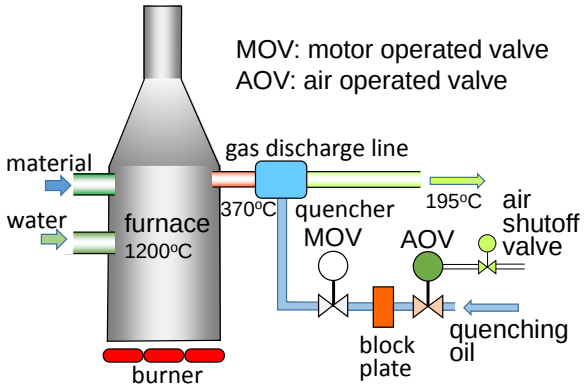

Fig. 12. Ethylene plant furnace and gas discharge line

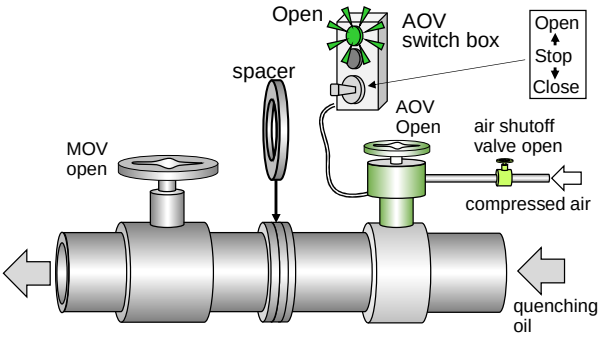

Fig. 13. Quenching oil control during normal operation

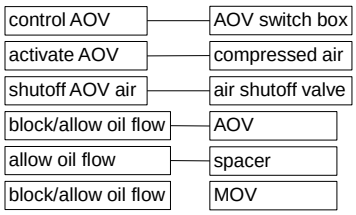

Fig. 14. DRG elements of the quenching oil line

During the maintenance of the furnace tubes, a block plate is inserted in place for the spacer so the quenching oil has no chance of reaching the quencher. The process of exchanging the spacer with the block plate had double protection against accidental quenching oil leakage. The air shutoff valve was closed so the air-operated valve (AOV) will not accidentally open and even the AOV itself was locked so that it will not open during the exchange as Fig. 15 shows.

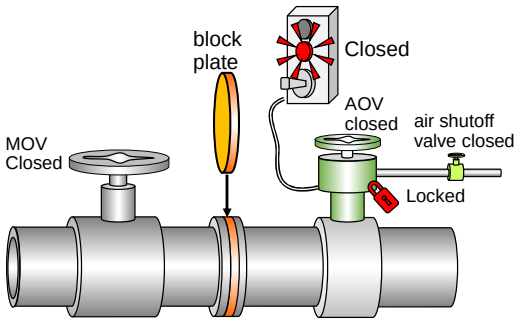

Fig. 15. Quenching oil control valves during plate/spacer exchange

3.2 The Accident

Equation (3) shows the design equation for the elements in Fig. 15 upstream of the block plate. Note that the equation looks like a clean uncoupled design without inclusion of human factors.

$$\begin{Bmatrix} \text{show AOV closed} \\ \text{lock AOV} \\ \text{shutoff AOV air} \\ \text{block oil flow} \\ \text{disable oil flow} \end{Bmatrix} = \begin{bmatrix} X & 0 & 0 & 0 & 0 \\ 0 & X & 0 & 0 & 0 \\ 0 & 0 & X & 0 & 0 \\ 0 & 0 & 0 & X & 0 \\ 0 & 0 & 0 & 0 & X \end{bmatrix} \begin{Bmatrix} \text{AOV switch box} \\ \text{physical lock} \\ \text{air shutoff valve} \\ \text{AOV closed} \\ \text{block plate} \end{Bmatrix} \quad (3)$$

On the day of the accident, preparing the quenching oil line for the decoking process went without trouble, however, there is no record of whether the procedures were properly followed. The accident broke out after the decoking was complete and when the operators were preparing the quenching oil line for the next thermal decomposition process.

The double protection for preventing quenching oil leakage were broken; the air shutoff valve was open and the physical lock on the AOV was not in place. If the situation was just so, the accident could have been avoided, however, an unfortunate event took place.

The heavy block plate had to be lifted out of place using a chain hoist. Figure 16 shows a chain hoist with an operator hoisting up the block plate.

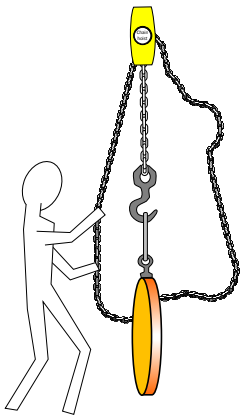

Fig. 16. Imaginary sketch of operator hoisting the block plate

Anyone who has operated one or seen one in operation knows that the hand chain that the operator keeps pulling can swing and swish around like a whip. The swinging hand chain swished toward the AOV switch box and happened to hit the switch in the direction to open the AOV. Without its physical lock and the air shutoff valve open, the AOV started to open and the quenching oil gushed out of the pipe where the block plate used to be.

Then for an unknown reason, the oil caught fire and put the two operators lifting the block plate in flame. There were two other workers downstairs for a different job and they were suddenly covered with flaming oil.

3.3 The Cause

The cause of the accident were the following three points:

(1) Air shutoff valve was not closed and air line was not purged

(2) Physical lock on the AOV was not in place

(3) The hand chain of the chain hoist happened to hit the AOV switch box to open the AOV

An investigation by the company revealed that the field knew that the air shutoff valve had to be closed, the line purged, and the physical lock had to be installed on the AOV. The information, however, were not well documented and not relayed to the contractors in the field. Relying on memory for following important procedures should be avoided by any means in the field.

4 Human Factors in AD

4.1 Adding Human Factors in DP

Accidents should be avoided, however, without simple ideal ways of doing so, accidents keep repeating. In Section 3, we discussed how relying on memory can be a serious cause of accidents. Section 2 also explained how simple operations of machines rely on eyes, ears, and hands of human operators.

This paper proposes to include typical human factors in AD analysis so people can identify reliance on human of their processes and systems. The factors to add are: eyes, ears, hands, and for the brain, reasoning and memory. The worst of all to rely on is the brain memory. Even a sound person with good reasoning can happen to forget important steps in work. Steps in operation better be procedural, i.e., specified in procedure documents or checklists than relying on memory. So, we also added "procedural" as a DP to the design equation and revised Eq. (3) as follows:

$$\begin{Bmatrix} \text{show AOV closed} \\ \text{lock AOV} \\ \text{shutoff AOV air} \\ \text{block oil flow} \\ \text{disable oil flow} \end{Bmatrix} = \begin{bmatrix} X & 0 & 0 & 0 & 0 & X & 0 & 0 & 0 & 0 & 0 \\ 0 & X & 0 & 0 & 0 & 0 & 0 & 0 & X & 0 & X0 \\ 0 & 0 & X & 0 & 0 & 0 & 0 & 0 & X & 0 & X0 \\ 0 & 0 & 0 & X & 0 & 0 & 0 & X & 0 & 0 & X \\ 0 & 0 & 0 & 0 & X & 0 & 0 & X & 0 & 0 & X \end{bmatrix} \begin{Bmatrix} \text{AOV switch box} \\ \text{physical lock} \\ \text{air shutoff valve} \\ \text{AOV closed} \\ \text{block plate} \\ \underline{\text{eyes}} \\ \underline{\text{ears}} \\ \underline{\text{hands}} \\ \underline{\text{reasoning}} \\ \underline{\text{memory}} \\ \underline{\text{procedural}} \end{Bmatrix} \quad (4)$$

4.2 How the Procedure Could Change

Blocking the oil flow by closing the AOV and disabling the flow with the block plate are steps for the process itself so they are procedural. The problem was relying on memory for the AOV air shutoff and the physical lock. We will discuss here the types of possible solutions and their effects in the remainder of this section.

4.2.1 Covering the AOV Switch Box

One of the solutions the plant implemented was to cover the switch box in a case [4]. This solution is quite effective because it blocks reason (3) in Section 3.3.

4.2.2 Documenting the procedures

In dealing with the other two reasons, the plant included the processes in their documents and further raised awareness in the field [5].

The efforts shifted the memory reliance to procedural thus the two Xs in the second last column of Eq. (4) are now moved to the right as Eq. (5) shows.

$$\begin{Bmatrix} \text{show AOV closed} \\ \text{lock AOV} \\ \text{shutoff AOV air} \\ \text{block oil flow} \\ \text{disable oil flow} \end{Bmatrix} = \begin{bmatrix} X0000X00000 \\ 0X00000X0\mathbf{0X} \\ 00X0000X0\mathbf{0X} \\ 000X000X00X \\ 0000X00X00X \end{bmatrix} \begin{Bmatrix} \text{AOV switch box} \\ \text{physical lock} \\ \text{air shutoff valve} \\ \text{AOV closed} \\ \text{block plate} \\ \underline{\text{eyes}} \\ \underline{\text{ears}} \\ \underline{\text{hands}} \\ \underline{\text{reasoning}} \\ \underline{\text{memory}} \\ \underline{\text{procedural}} \end{Bmatrix} \quad (5)$$

We, however, still see problems in this solution when we think of the work environment of today. Work procedures and manuals are typically shelved in offices and work scheduled for the day are possibly reviewed at the start of the day. Careful workers may take copies of relevant pages to the field. Although the solution is much better than relying on memory alone, there are some limitations.

4.2.3 Interlocking

Large scale plants, like the chemical plant in this paper, or nuclear plants typically have interlocks to prevent disastrous operations by operators that are novices or were absent minded. They are quite effective because they disable unwanted movements. The problem is, however, they require cost and man-power to implement, and sometimes are not really feasible.

For example, let's say the plant decided to put an interlock so the bolts on the block plate flange cannot be loosened without closing the AOV shutoff valve and purging the line. Monitoring the status of a mechanical part is easy, however, blocking mechanical operation on physical parts is different from disabling an electrical pushbutton on the control panel. If possible, however, it is an ideal solution.

4.2.4 Solution with (Internet of Things) IoT

As we stated in the previous Section 4.2.3, monitoring status of mechanical parts is relatively easy. Thus, checking whether the air shutoff valve is open or not and whether the air line is purged or not are accomplished with a position or touch sensor and a pressure sensor. We can send these signals to an online system.

Another trend that we are starting to see and probably will be a major practice in the future is to readily have the manual on-site at the field, on the spot of operation. Carrying a PC to the spot is probably difficult, however, a tablet or a smartphone is easy to carry around. Operators can check the manual for procedures of their task while they are working.

Adding this technology to signals from statuses of crucial parts, we can notify operators if the system is ready for the next step or they have other tasks to clear before it.

Mechanically interlocking loosening of the bolts that hold the block plate in place is difficult, however, sending a confirmation if the system is ready for loosening the bolts or not is feasible.

5 Conclusions

We showed that human factors are usually left out from conceptual designs. We showed how we can incorporate them into DRG and design equations with AD.

Human factors left out from conceptual design tend not to pose serious threats to product safety during normal operation. Maintenance work, on the other hand, has serious reliance on human factors and not recognizing the burden on workers could lead to accidents. In such cases, it is easy to blame the operator, however, we need to identify excessive reliance on human before such accidents take place.

We showed how we can identify how systems rely on human by including, "eyes," "ears," "hands," "reasoning," and "memory" into the DP vector of AD.

Relying on human memory is a bad practice in operation and we added a DP element "procedural" so that when reliance on human memory are found, managers can make efforts to shift them to procedural reliance.

We believe that manuals and procedural documents will be readily carried around in the field in the future, and when critical parts can send their statuses to online systems, the electronic documents can notify operators if steps they are about to make are appropriate or not.

References

1. N.P. Suh, *Axiomatic Design, Advances and Applications* (2001)
2. K. Iino, and M. Nakao, Design Record Graph and Axiomatic Design for Creative Design Education, *ICAD 2016* (2016)
3. Mitsubishi Chemical Corporation, I. Summary and Causes of the fire accident, from Fire at the Kashima Plant No. 2 Ethylene Plant, https://www.m-chemical.co.jp/en/csr/kashima.html (accessed May 13, 2018)
4. Mitsubishi Chemical Corporation, III. Status Report of Measures for preventing a recurrence, from Fire at the Kashima Plant # 2 Ethylene Plant, Oct., 2008, https://www.m-chemical.co.jp/csr/pdf/kashima_j03.pdf (accessed May 13, 2018)
5. Mitsubishi Chemical Corporation, II. Measures for preventing a recurrence, from Fire at the Kashima Plant No. 2 Ethylene Plant, Mar., 2018, https://www.m-chemical.co.jp/en/csr/kashima.html (accessed May 14, 2018)