Handout 4: Linear & Complex Accidents

We have considered six questions

> **Q1:** How can we avoid error, decrease the number and seriousness of accidents?
> **Q2:** With a fairly high degree of forethought and inquiry, can we anticipate *all* of the *serious* accidents that might result from using technology?
> **Q3:** What is the *primary cause* of accidents?
> **Q4:** What types of benefits do complex, high-risk technologies expose us to?
> **Q5:** Do the benefits of using complex, high-risk technologies outweigh the risks?
> **Q6:** Why haven't there been *more* catastrophic accidents or TMIs?

One thesis of Perrow's book is that there is a unique kind of accident called "system (normal) accident." This type of accident is not attributed to the designers, owners, or operators of the technology, but instead applies to the complex technological system itself (i.e., it is due to the fact that a technological system has many parts that interact in unexpected and unpredictable ways).

If we want to understand what this means, how to respond to it, and if we want to use this idea to think about other technologies, we need to get clearer about some of the terms involved.

1. Accident, System, Subsystem, Unit, Part

Let's begin with the definition of an *accident*.

> D1: "an unintended and untoward event" (Perrow, p.63)
> O1: When we use the term "accident", we want to reference that something bad happened. Some damage or someone or something was hurt:
>
> D2: "an unintended and untoward event" (Perrow, p.63) that involves "some damage to people, objects, or to both" (Perrow, p. 64)
> O2: This is a bit unclear. The notion of an accident should refer to the disruption of a future task since slightly scratching my car while driving isn't an "accident."
>
> D3: "an unintended and untoward event" (Perrow, p.63) that involves "some damage to people, objects, or to both" that is "sufficient to disrupt the ongoing "task" or future tasks that will be demanded of the objects or people" (Perrow, p. 64)
> O3: Not all disruptions are of the same degree. We need a way to distinguish between major and minor disruptions and to the part of the system they impact.

4th level	accident	*system* (array of subsystems, e.g. nuclear plant)
3rd level	accident	*subsystem* (array of units, e.g. steam generator and cooling system)
2nd level	incident	*unit* (collection of parts that serve one function, e.g. steam generator)
1st level	incident	*part* (smallest item that can be disrupted), e.g. valve

D4: An *accident* is a failure in a subsystem or system where there is damage to more than one unit and this damage disrupts the ongoing or future output of the system.
D4*: An *incident* is damage that is limited to parts or a unit, regardless whether it disrupts the ongoing or future output of the system.[1]

Note: In writing your paper, you want to clearly define what you mean by "accident" and "incident" & you will want to indicate whether it pertains to the whole system, the subsystem, the unit, or the part.

2. Victims

Let's distinguish between different victims.

Type of Victim	Example
first-party victims	operators (those with influence on the system), e.g. pilots, laborers in a steel mill, drivers, phone users, et al.
second-party victims	nonoperating system users (they use the system but have no influence on the system), e.g. airline passengers, individuals who work (even if they only do clerical work) at a refinery. These individuals are not completely innocent as they know the risks of using the technology.
third-party victims	innocent bystanders, individuals with no involvement in a system (e.g. being hit by a plane).
fourth-party victims	fetuses and future generations, e.g. victims of radiation, toxic chemicals

Perrow rejects the idea that just because we live near a high-risk technology (e.g. a nuclear plant) means that we are not innocent bystanders. That is, living near a nuclear plant means that we are second-party victims rather than third-party victims. His argument runs something like this:

PROXIMITY DOES NOT IMPLY INVOLVEMENT.

P1 There is no *practical* means of avoiding being within 50 miles of a nuclear reactor.
P2 Even if we could be farther than 50 miles from a nuclear reactor, certain weather conditions could contaminate areas more than 200 miles, e.g. if the weather conditions were right.
P3 We can only be seen as second-party victims if we use, are associated with, the technological system.
C Therefore, those with no practical means of avoiding being near a reactor are not second-party victims.

CDQ: Do you agree with Perrow when he claims that proximity to a high-risk technology does not mean that you are involved with it? That is, just because you are *in* a society that *uses* a certain technology (and perhaps you even use it to some extent) does not mean that you *assume the risks* of being hurt were that technology to fail.

Now let's gauge our reaction to individuals hurt in the use of a technology

[1] Perrow, p.66.

Type of Victim	
first-party victims	individual killed while driving a bus
second-party victims	individual killed as a passenger on a bus
third-party victims	individual killed because they were hit by a bus
fourth-party victims	fetus killed because the pregnant mother was hit by a bus.

Perrow contends that "[f]orth-party victims potentially constitute the most serious class of victims" (p.69).

- certain genetic defects to future persons are life-long and can diminish one's life
- certain genetic defects create an additional burden, e.g. lifetime care by parents or the State
- ignoring the seriousness of harm is indicative of selfishness: "[f]uture generations carry the burden; the present generation reaps whatever rewards there may be from the activity" (p.70)

CDQ: Do you agree with Perrow when he says that fourth-party victims are the most serious class of victims? If you do, explain how this should impact our use and development of technologies? If not, explain why the reasons Perrow gives for his view are mistaken.

Note: In writing your paper, you want to clearly indicate who the relevant (or most serious) victims are (first-party, second-party, ...) and *why* they are relevant (e.g. see the reasons given above)

3. Component Failure Accidents, System Accidents, Final Accidents

Let's distinguish between two different kinds of accidents/incidents according to whether or not we can anticipate them.

Component failure accidents are failures that involve one or more components of the system (part, unit, subsystem) that are linked in an *anticipated* sequence. Component failures are thus expected or comprehensible to those who designed the system. They are failures we can say "oh, I can see how this might happen and so we have to think about whether or not to build a redundancy to ensure that damage is limited.

System accidents are failures that involve *unanticipated* interaction of multiple failures. These are failures that involve multiple failures and are unexpected to those who designed the system. They are failures that we don't foresee happening, not because we say "oh that could happen but it isn't likely" but that we say "oh, I never even thought that would occur."

Final accidents are large-scale accidents that we might be able to anticipate but they are so rare (or so devastating) that it is somewhat pointless to really develop redundancies. There is also no way for the operators of the technology to reduce the damage from the accident. For example, if a meteor hit a nuclear power plant, the sun exploding, a commercial plan being shot out of the sky by a rocket, etc.

Accidents	Final	Least frequent
	System	infrequent
	Component	More frequent
Incident	Incident	Least frequent

CDQ: On 11 March 2011, the Fukushima nuclear power plant was hit by a tsunami that was triggered by an earthquake (Japan is located in an active seismic zone). The Fukushima facility was composed of six boiling water reactors (BWRs) of two different designs (by GE) and operated by the Tokyo Electric Power Company (TEPCO). On March 11, reactor 4 was defueled while reactors 5 and 6 were shut down for maintenance. Immediately after the earthquake, the operating reactors automatically stopped the fission reaction in the reactor (SCRAMmed). However, while fission ceased in the reactor, the reactor fuel still produces decay heat and so must remain active for several days (i.e. just because the reactor is turned off doesn't mean it's "off" as it can still meltdown from the heat produced by the reaction). With the reactor SCRAMmed, two emergency diesel generators powered the plant's electronics and cooling system. 50 minutes later, the 14 meter tsunami went over the 10 meter seawall. The water flooded the low-lying room containing the diesel generators causing them to shut down and back-up emergency battery power to activate. Three additional backup generators were available at higher-ground were activated but the switching stations (stations that transmit the electricity from the back-up station) were also flooded (they weren't watertight) and so the plant switched to its 8-hour back-up *battery* power). Individuals rushed to provide additional back-up battery power, but transportation was exceedingly difficult due to poor road conditions. The battery power ran out after a day, the reactor began to heat up and there were multiple hydrogen-air explosions in all three reactors.

In the course of the accident radioactive gas was released. A 2013 WHO report says that for infant girls exposed to the radiation in the most affected areas, there is a 70% higher risk of developing thyroid cancer, a 7% higher risk of leukemia for infant males, and a 6% increased risk of breast cancer in females. In addition, 2 years after the accident, it was discovered that 300 tons of radioisotope-contaminated water leaked from a storage tank into the Pacific Ocean. This was initially denied by TEPCO but was later confirmed once the Japanese Prime Minister ordered an investigation.

What type of failure would you characterize the Fukushima accident as (accident or incident?, final, system, or component?) Who are the most relevant victims?

Note: In writing your paper, you want to clearly indicate what kind of accident you are considering and then if you are dealing with the risks associated with that accident, you might consider whether or not the accident can be prevented.

4. Linear and Complex Reactions

A linear interaction is a series of events that can be laid out in a straight-line, e.g. an assembly line. For example, suppose we have a process designed to produce a product. It is assembled in a series of events:

A to B to C to D to E to F to product.

Now suppose that there is a problem in the chain, e.g. in the transition from D to E. If the process is allowed to continue, then A will pass to B, B to C, C to D, and then we will have a piling up process in the transition from D to E. To fix this, we simply stop the process, fix the transition from D to E, then restart the process. In the linear reaction each part *only has one function*. A's function is to pass to B, B's function is to pass to C, and so on.

In non-linear interactions, parts have multiple functions. Here is a simple example.

A	B	C
D	E	F
G	H	I

Let's suppose that if a letter is connected to another letter (adjacent or diagonally), then the letter interacts with that letter. For example, A interacts with B and D, while D interacts with A, B, E, H, and G. A concrete example is given by Perrow when he points to a heater that (i) heats the gas in a tank and (ii) absorbs excess heat from the reactor.

Now let's suppose that **not ALL** of the interactions produce a product, but **SOME** combination of them. That is, some of the interactions are **designed** while others are possible but don't really play a key role in producing the product. For example, E *could* interact with C (simply because it is *close* to it, what Perrow refers to as *proximity*), but it isn't one we are particularly concerned with. Perrow contends that one of the key ingredients to system accidents is that they often involve an "unanticipated connection between two independent, unrelated subsystems that happened to be in close proximity" (p.74). There interaction was "certainly not a planned, expected, linear one" (p.74).

The basic idea seems to be that linear accidents are *visible*. We designed the assembly line in a certain way and so if there is a problem, we can scan the line, see the problem, and correct the mistake. However, in the case of system accidents (non-linear accidents) some of the interactions are not designed and so if there is a problem, it is unexpected and isn't always visible. We have to investigate what the problem is. *But this takes time!*

CDQ: Consider the example from pp.73-74 concerning the Dauntless Colocotronis. Try to explain how this is an example of a complex non-linear reaction

5. Linear or Complex Systems

Let's consider an earlier argument.

ARGUMENT FOR **SAFER** CATASTROPHE-PRODUCING COMPLEX TECHNOLOGIES

P1	If some complex technological systems are likely to produce rare but unpredictable catastrophic events, then we should **make the existing systems safer.**
P2	Complex technological systems are likely to produce rare but unpredictable catastrophic events.
C	Therefore we should **make the existing systems safer.**

According to Perrow, one way that we can make technologies safer is by **making them more *linear*.**

	Pros	**Cons**
Linear	Safer, less complex, problems are easier to diagnosis, tend to be slower, parts can be isolatable, typically more understanding of how the parts interact	Less efficient, more costly, we don't know how to make some technologies completely linear
Complex	Since parts / components serve multiple functions, they are more efficient, take up less space, cheaper	More dangerous, problems are harder to diagnosis, some interactions are unknown

Example #1: You have a single control room that governs five different nuclear power plants. It receives information from each plant, then sends commands to each plant. Suppose there is an earthquake, and it damages a component in the control room. This causes a command to be sent out to *some* of the reactors to speed up the reaction (creating more heat). But as this is a complex reaction, we have the problem of whether there is a *problem* at the reactors (A, B, C) or in the control room. We don't know whether the problem is in one of the reactors A, B, and C or in the control room (4 locations). If you had a single control room for each reactor, then there are only 2 locations to check.

Example #2 (non-technological): I designed this course, teach you the material (or at least try), and grade your work. I'm one part playing *multiple functions* in a complex interaction. Suppose that I *rightfully* give you all 100% on your exams. It then might be thought that I'm *inflating* the grades! Suppose then I am promptly fired (the accident!). This accident would be the result of a *difficulty* in diagnosing what happened when I gave you a 100% (and general skepticism that anyone could be that great of a teacher).

The system might be made more linear (and the accident avoided) by (i) A designing the course, (ii) B teaching the course, and (iii) C grading the work. If A, B, and C were all segregated, had limited interaction with each other, but A simply passed B the course, B taught the course, and C grades the work, then if B's students all receive 100%, then B likely would not be fired.

CDQ: Think of some way to make a complex technology (or any complex interaction, it can be an organization) more linear. Come up with an example.

Note: In writing your paper, if you have a positive proposal for making at technology/process safer, rather than simply building in multiple redundancies, you might consider a proposal for how the technology might be made more linear. However, keep in mind that, in a lot of cases, making a technology/process more linear often means making it more expensive.