Systemic accidents from a resilience engineering perspective

Erik Hollnagel[1,2]

1 *1 Institute of Regional Health Research – University of Southern Denmark*
2 erik.hollnagel@rsyd.dk

In a historical way safety has been defined by its opposite, since its improvement has been measured by the *reduction* of safety-related events. In other words, safety has been measured by the '*lack of safety*'. The European Technology Platform on Industrial Safety (2005) gives a good example of this view by stating that industrial safety performance will progress in a steady and measurable way reducing accident-related losses, occupational diseases and environmental incidents.

Other domains adopt similar definitions. Take aviation, for example, with the International Civil Aviation Organization [ICAO] defining safety as a state of reduced harm to persons or of property, at or below an acceptable level through continuous hazard identification and risk management processes (ICAO, 2013). Indeed, a generic definition of safety could be something like 'The freedom from unacceptable risk'. However, risk, damage, and accidents do not represent safety. They do represent lack of safety, instead.

Such definitions of safety have two important practical consequences. First, safety management focuses on what goes (or might go) wrong aiming to prevent it and/or limit its consequences and, second, safety indicators express adverse outcome figures; i.e., things that went wrong. Safety is thus, measured by the consequences of its absence, rather than by a positive quality indicator.

Why are we looking at the wrong place?

Adverse events and their outcomes are mostly unexpected, hindering purposive human activity, whether at work or at leisure. These surprising events prevent us from achieving individual and collective goals. Therefore, all trials to avoid them to happen make sense. In practice, we want to *be* safe – in the sense of being sure an adverse event will not happen (at least, not very often) –, and to *feel* safe – in the sense of having an explanation when an adverse event happens. Ultimately, accidents threat the basic human need for feeling safe since they represent uncertainty.

Both needs of *being* and *feeling* safe can be satisfied through the explanation of *why* something has happened, which is tantamount to finding a cause. Yet causes of bad events are never *found* but *built*. Causes are socially agreed – or acceptable – explanations for events. Therefore, they reflect the prevailing culture and the current level of development. In ancient times, acceptable causes were '*acts of god*' or '*forces of nature*'. As civilisations matured and humans started to master the environment, causes were found in technological failures and malfunctions – particularly after the industrial revolution during the 18th century. In the late 1970s, human actions – and 'human error' – became the preferred cause. In the mid-1980s, this was surpassed by safety culture, which recently has started to give way to the notion of 'complex adaptive systems.'

Just as the contents of explanations have changed over time, so did have the manifestations of accidents, with regard to type, frequency, and magnitude of consequences. Before the industrialization of societies, accidents had local consequences, mostly affecting those directly involved with the risks. Systems were tractable (cf below). The tempo was shorter and technology simpler, leading to visible consequences. Therefore, shallow explanations were often sufficient.

In the 21st century, the conditions are radically different, as many systems have become intractably complex. The tempo has expanded and technology is often intricate, resulting on latent and manifest consequences. Therefore, simple explanations are no longer enough.

However, while the preferred type of causes has changed, the basic way of thinking has not. There is still a preference for monolithic causes as well as for simple cause-effect reasoning. The common belief in causality is so strong that it corresponds to a *causality credo*, which represents the following 'logic':

a) Things that go right and things that go wrong have different causes. Unwanted outcomes (e.g. incidents and accidents) are consequences of things that went wrong, while successful outcomes are the results of 'normal' events;

b) Enough evidence collection will identify all causes of adverse outcomes. Once causes are identified, they can be eliminated, encapsulated, or otherwise neutralised; e

c) Considering that all adverse outcomes have a cause (or causes), and since all causes can be found, all accidents can be prevented.

While causality makes sense when reasoning along? a cause-effect logic, the *causality credo* misleads us into the opposite, making us believe that equal justification through reasoning backwards from effects can lead to the causes. Nevertheless, it cannot.

Today, safety management is? Facing much larger and complex systems than in the past. There are many more details to consider and operation modes to know. There may be tight and partly unrecognised couplings amongst functions, and the whole system is under constant change while being described. For some systems, it is clearly not possible to prescribe tasks and actions in every detail, and we

must therefore relinquish the notion that *work-as-imagined* will correspond to *work-as-done*.

On the other hand, the basement of work success is flexible rather than rigid performance. In fact, the less thoroughly? A system is described, the more performance variability is needed.

Understanding the challenge of systemic accidents may be easier through the distinction between tractable and intractable systems (Hollnagel, 2011). The former systems can be completely described or specified, while the latter cannot. Table 1 summarizes the differences between the two types of systems.

Tractable system administration assumes that workplaces are well-designed and correctly maintained, while procedures are comprehensive, complete, and correct. People, at the sharp end, will behave as planned because they were trained to. System designers have foreseen every contingency and have provided appropriate response capability to the structure.

Intractable system administration must accept that systems cannot be decomposed in a meaningful way because there is no natural 'elements' or 'components'. Procedures and guidelines will never correspond precisely to the actual situation; and day-by-day performance is — and must be — flexible and variable.

Table 1: Tractable and Intractable Systems

	Tractable System	Intractable System
Number of details	Descriptions are simple (few details)	Descriptions are elaborate (many details)
Comprehensibility	Principles of functioning are known	Principles of functioning are partly unknown
Stability	System does not change while being described	System changes before description is finished
Relationship with other systems	Independent	Interdependent
Work organization	Stable, tasks are regular and can be prescribed	Unstable, tasks must adjust to match the conditions, and cannot be prescribed
Internal links	Linear, outcomes are resultant	Non-linear, outcomes are emergent

Well-established safety management methods have been developed over the assumption that systems are tractable. Since this assumption is generally? No longer valid, new methods to deal with intractable systems and irregular work environments are necessary. One option to do that is through the focus on how work activities are organized in relation with the current situation (e.g. existing resources and demands). In other words, we should look at? How things go right rather than how they go wrong, making a clear distinction between two ways of viewing safety, called Safety-I and Safety-II, respectively.

According to Safety-I, a system is safe when there is no accident or incident. Then, safety-related activities have the purpose of preventing things going wrong, to the extent possible. According to Safety-II, a system is safe when it is resilient, which means it can 'adjust its functioning prior to, during, or following changes, disturbances, and opportunities, so that it can work under both expected and unexpected conditions' (Hollnagel *et al.*, 2011). Then, safety-related activities have the purpose of making things go right, as much as possible.

Safety-I and Safety-II do not differ in their overall goal, which in either case is the avoidance of adverse events whenever possible. But, whereas Safety-I tries to achieve this by eliminating what can go wrong, Safety-II tries to achieve it by facilitating everyday work, by improving the system's resilience and thereby ensure that things go right as much as possible.

Resilience Engineering and Safety-II agree on their view on safety. The best way to ensure a safety system is not exclusively through preventing relatively few cases in which something may go wrong. Instead, the best way is through facilitating everyday successful performance as frequently as possible. Instead of conducting investigations after infrequent accidents or striving to reduce adverse outcomes, safety management should allocate resources to look at the positive events trying to learn from them. Rather than learn based on severity, people should learn from events based on their frequency. Likewise, instead of analysing single severe events in depth, people should explore the regularity of the many frequent events in breadth, to understand the patterns in system performance.

Rather than incompatible or conflicting approaches, Safety-I and Safety-II represent complementary views of safety. Therefore, many existing practices can still be used with different emphasis. The transition to a Safety-II perspective will however emphasise some new types of practices.

In summary?, look at what goes right as well as what goes wrong, and learn from both. Do not wait for something bad to happen; try to understand what actually takes place in situations where nothing out of the ordinary seems to happen. Finding out why things go well and trying to learn from them is at least as important as finding the causes of adverse outcomes.

Seek for what happens regularly and focus on events based on their frequency rather than on their severity. Small continuous improvements in everyday performance may be more significant than a large improvement of exceptional performance.

Although Safety-II focuses on things that go right, it is still necessary to keep in mind that things can also go wrong and it is necessary to 'be aware of the possibility of failure'. However, the 'possible failure' is not only something related

to ‘malfunction’ as under the Safety-I view, but also that we forget to facilitate everyday successful activities.

Do not prioritise efficiency over completeness. If most of the time is spent trying to make ends meet, there is little or no time to consolidate experiences. Improvements must be legitimate within the organisational culture in order to allocate resources – especially time – to reflect, to share experiences, and to learn. If that is not the case, then how can anything ever improve in a permanent way?

LIST OF REFERENCES

European Technology Platform Industrial Safety [ETPIS]. (2011) Safe Future Approach, Vol. 24, July 2011.

Hollnagel, E. (2011). RAG – The Resilience Analysis Grid. In: E Hollnagel, J Pariès, DD Woods & J Wreathall (Eds). (2011) *Resilience engineering in practice: a guidebook*. Farnham, UK: Ashgate.

International Civil Aviation Organisation [ICAO]. (2013) Safety Management Manual [SMM], Doc 9859-AN474, 3rd Edition, Montreal, Quebec, Canada.