What should we look at and what should we learn from?
A Resilience Engineering / Safety-II perspective

Erik Hollnagel
Professor
University of Southern Denmark

hollnagel.erik@gmail.com

Chief Consultant
Center for Quality, RSD (DK)
Thinking about safety

We usually think about safety in relation to incidents and accidents: low probability events with adverse outcomes.

A system is safe if as little as possible goes wrong.


© Erik Hollnagel, 2017
We need to **be** safe and to **feel** safe

Accidents, incidents, breakdowns, disruptions.

A need to **be** safe (explanations)

A need to **feel** safe (assurances)

“Acts of god” ➔ Technical failures ➔ Human Factors ➔ Safety culture ➔ Complex systems

When looking for explanations, we have a preference for single (monolithic) causes

© Erik Hollnagel, 2015
Monolithic explanations

Monolithic explanations: rely on a single concept or factor. Monolithic explanations: are social constructs. Monolithic explanations: are an ETTO.

They are efficient (easily found and explain). But they lack in thoroughness and in precision.

<table>
<thead>
<tr>
<th>Type of explanation</th>
<th>Main use:</th>
<th>Typical recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Human error” (human factor)</td>
<td>Accidents (individual)</td>
<td>Eliminate or prevent (e.g., compliance)</td>
</tr>
<tr>
<td>Situation awareness</td>
<td>Loss of control (individual)</td>
<td>Enhance or support (e.g., display design)</td>
</tr>
<tr>
<td>Safety culture</td>
<td>Accidents (organisational)</td>
<td>Improve or increase (Safety Journey)</td>
</tr>
<tr>
<td>Complexity</td>
<td>Loss of control (organisational)</td>
<td>Transform / match (system design, training)</td>
</tr>
</tbody>
</table>
90.3% of crashes involved human error, such as risky driving behavior, inadvertent errors, and impaired states. (Foundation for Traffic Safety (2006)

More than seventy percent of all crashes of scheduled aircraft are caused directly by ‘controlled flight into terrain’. FAA (2001)
How to feel safe

The belief in causality (Causality Credo)

(1) Adverse outcomes happen because something has gone wrong (cause-effect thinking + value congruence between cause and effect).
(2) Causes can be found and treated (rational deduction).
(3) All accidents are therefore preventable (zero harm principle).

ZEROMindset
We believe that all injuries and occupational illnesses are preventable.
We are responsible for preventing and correcting unsafe behaviour and work conditions.

NOREpeats
All unsafe practices and incidents will be investigated to determine what happened and why.
All necessary steps will be taken to prevent recurrence.

SIMPLE Non-negotiable standards
We will adopt a common, simple set of non-negotiable standards and rules throughout the Group.
Divisional line management at all levels has the responsibility of implementing and maintaining the standards and rules.
Increasing safety by reducing failures

Function (work as imagined) \[\rightarrow\] Success (no adverse events) \[\rightarrow\] Acceptable outcomes

Identification and measurement of adverse events is central to safety.

Malfunction, non-compliance, error \[\rightarrow\] Failure (accidents, incidents) \[\rightarrow\] Unacceptable outcomes

“Find-and-fix”
Safety-I – when nothing goes wrong

Safety is a condition where the number of adverse outcomes (accidents / incidents / near misses) is as low as possible.

Safety-I is defined by its opposite - by the lack of safety (accidents, incidents, risks).

The premise for Safety-I is the need to understand why accidents happen.

Accidents and incidents are situations that, by definition, lack safety.

How can we improve safety by studying situations where there is NO safety?
Managing safety by snapshots

Harmful events attract attention. But they are rare and isolated.

Events are analysed step-by-step and part-by-part. Prevention/responses are developed for each problem found.
What do we learn from?

“We were moving the single man-lift with 4 men. The lift would not fit through the door standing up and we began to tilt the lift parallel to the ground when the lift was 6 inches from the ground it slipped and crushed Sam’s finger subsequently taking it off.”

“Lessons learned”

Failed to read operating manual, and practice transport and movement. Failed to follow operating manual. Failed to heed warnings, cautions, etc. affixed to equipment and in manual. Failed to wait for Superintendent to determine safe procedure. Directed other workers in potentially dangerous manner.
Wrong Blood in Tube (WBiT)

WBİTs are estimated to occur at a rate of approximately 1 in 2,000 samples. Main causes are:

- labelling of sample tubes away from the bedside
- failure to check patient identity
- similar names (together with incorrect identity checks)
- use of pre-printed labels
- confusion of patient notes and/or request forms
- inaccurate verbal instructions/no request form

Environment (3 recommendations)
Staff (9 recommendations)
Equipment (12 recommendations)
Patient (2 recommendations)
Procedure (6 recommendations)
Culture (8 recommendations)

Altogether 40 recommendations.

These recommendations will provide input for those responsible for reducing errors related to mislabelling and miscollection of blood samples.
The implementation should be considered in the broader context of the organisational culture of Australian healthcare.

www.vmia.vic.gov.au
The first interpretation of safety

Safety is the prevention of harm to patients

\[ \text{Safety} = \sum_{i=1}^{n} \text{Accident}_i \]

There is an presence of failures (things that go wrong) due to risks and hazards. The number of harmful events can be counted.

It is “easy” to count how much goes wrong, but does that measure safety?

AHRQ Patient Safety Indicators (PSIs)

- **PSI 04** Death among surgical inpatients with serious treatable complications.
- **PSI 06** Iatrogenic pneumothorax.
- **PSI 11** Postoperative respiratory failure.
- **PSI 12** Postoperative PE or DVT.
- **PSI 14** Postoperative wound dehiscence.
- **PSI 15** Accidental puncture or laceration.
Managing Safety-I

Safety-I is a condition where the number of adverse outcomes (accidents / incidents / near misses) is as low as possible.

The belief in causality (Causality Credo)

1. Adverse outcomes happen because something has gone wrong (cause-effect thinking + value congruence between cause and effect).
2. Causes can be found and treated (rational deduction).
3. All accidents are therefore preventable (zero harm principle).

We are safe if there is as little as possible of this.

Prevent, eliminate, constrain. Safety, quality, etc. are different and require different measures and methods.
Do we really know how the system works?

The result of safety-I management is that we know something about what goes wrong, but almost nothing about what goes right!

We don’t know what happens here

We know what happens here

We know what happens here

We know what happens here
What should we be looking for?

Adverse outcomes = Absence of safety

10^{-4} := 1 failure in 10,000 events

Easy to see
Complicated aetiology
Difficult to change
Difficult to manage

‘Difficult’ to see
Uncomplicated aetiology
Easy to change
Easy to manage

Intended outcomes = Presence of safety

1 - 10^{-4} := 9.999 “successes” in 10,000 events
The second interpretation of safety

Safety is the prevention of harm to patients

\[ \text{Safety} = \sum_{i=1}^{n} \text{Accident}_i \]

There is an **presence** of failures (things that go wrong) due to risks and hazards. The number of harmful events can be counted.

"Safety is a dynamic non-event"

\[ \text{Safety} = \sum_{i=1}^{n} \neg \text{Accident}_i \]

There is an **absence** of failures (things that go wrong), but as a result of active engagement. If safety is a non-event, it can neither be observed, nor measured.

Is it possible to count the number of times something does not happen?
How do the non-events happen?

When we drive on the streets or move in a crowd, we continuously adjust our performance to what other people do.

Just as others continuously adjust to what we do – or will do.
How do we understand what happens?

Design (tools, roles, environment)

Work & production planning ("lean" - optimisation)

Safety management, investigations & auditing

Work-As-Imagined

Work-As-Imagined

Work-As-Imagined

Work-As-Imagined

Work-As-Done
Different ideas about why work is safe

Work is safe because … …

Why are there different ideas about why work is safe?

Work is safe because … …

Work is safe because … …

And how can they be reconciled?
Performance adjustments are necessary

Availability of resources (time, manpower, materials, information, etc.) may be limited and uncertain.

People adjust what they do to match the situation.

Performance variability is inevitable, ubiquitous, and necessary.

Because of resource limitations, performance adjustments will always be approximate.

Performance variability is the reason why everyday work is safe and effective. 😊

Performance variability is the reason why things sometimes go wrong. 😞
Increase safety by facilitating work

Understanding the variability of everyday performance is the basis for safety.

Function (work as imagined)

Everyday work (performance variability)

Malfunction, non-compliance, error

Success (no adverse events)

Acceptable outcomes

Failure (accidents, incidents)

Unacceptable outcomes

Constraining performance variability to remove failures will also remove successful everyday work.
Safety II – when everything goes right

Safety-II: Safety is a condition where the number of successful outcomes (meaning everyday work) is as high as possible. It is the ability to succeed under varying conditions.

Safety-II is achieved by trying to make sure that things go right, rather than by preventing them from going wrong.

- Safety is defined by its presence.
- The focus is on everyday situations where things go right – as they should.

Individuals and organisations must adjust everything they do to match the current conditions. Everyday performance must be variable in order for things to work.

- Acceptable outcomes
- Unacceptable outcomes

Performance variability
Thinking about safety

We should think about safety in terms of how many things go well and how frequently we succeed.

A system is safe if as much as possible goes right.
The third interpretation of safety

Safety is the prevention of harm to patients

\[ \text{Safety} = \sum_{1}^{n} \text{Accident}_i \]

There is a presence of failures (things that go wrong) due to risks and hazards. The number of harmful events can be counted.

“Safety is a dynamic non-event”

\[ \text{Safety} = \sum_{1}^{n} \neg \text{Accident}_i \]

There is an absence of failures (things that go wrong), but as a result of active engagement. If safety is a non-event, it can neither be observed, nor measured.

Safety is a dynamic event

\[ \text{Safety} = \sum_{1}^{n} (\text{acceptable outcome})_i \]

Safety is the presence of acceptable outcomes. The more there are, the safer the system is.
Resilience is an expression of how systems cope with everyday situations by adjusting their performance to the conditions. A system’s performance is resilient if it can function as required under expected and unexpected conditions alike (changes / disturbances / opportunities).

Resilience is not something a system has, but something a system does.
Resilience versus resilient performance

Resilience is an expression of how people, alone or together, cope with everyday situations - large and small - by adjusting their performance to the conditions.

Resilient performance means that an organisation can function as required under expected and unexpected conditions alike (changes / disturbances / opportunities).

Resilient performance requires that an organisation has the potentials to respond, monitor, learn, and anticipate.
As high as reasonably practicable

Respond

For which events is there a response ready?
What is the threshold of response?
How many resources are allocated to response readiness?
...

Monitor

How have the indicators been defined?
How many indicators are leading and how many are lagging?
What is the delay between measurement and interpretation?
....

Learn

What is the learning based on (successes – failures)?
Is learning continuous or event-driven?
How are the effects of learning verified and maintained?
...

Anticipate

What is the implicit/explicit “model” of the future?
How far does the organisation look ahead (“horizon”)?
What risks are the organisation willing to take?
...
The Resilience Assessment Grid (RAG)

Comprises four sets of questions, one for each potential. The questions are:
- **DIAGNOSTIC** – point to details of a potential that are meaningful to assess.
- **FORMATIVE** – answers can be used to make decisions about how to improve potentials.
- **SPECIFIC** – address issues that are important for a concrete organisation.
Resilience potentials are coupled
What should we care about?

Care about what happens all the time rather than what happens rarely.

The numerator is how many there are of a type of event – accidents, incidents, etc. This number is known (with some uncertainty).

The denominator is how many cases something went well. This number is usually unknown.

We always count the number of times something goes wrong. We analyse the rare events.

We rarely count the number of times something goes well. We need to understand the common events.
What should we be looking for?

Look for ‘work-as-done’ - the habitual adjustments and why they are made

In order to understand WHY this happened …

How do people create and maintain good working conditions?

How do people compensate for what is missing?

How do people avoid future problems?

… we need to understand HOW this happens!

When we notice something that has gone wrong …

... it is a safe bet that it has gone right many times before …

... and that it will go right many times in the future.
What should we learn from

Learn from what is frequent/regular, not from what is infrequent/irregular.

It is difficult – and expensive – to make large improvements of rare performance.

The effects of small improvements are easier to measure, and can be seen in both safety and productivity.
Management of Safety-II

Safety-II: Resilient safety management

1. Care about what happens all the time rather than what happens rarely. **We always count the number of times something fails, but rarely the number of times it just works.**

2. Look for ‘work-as-done’ - the habitual adjustments and why they are made. **When something is done, as a part of work, it has usually been done before and gone well before.**

3. Learning should be based on the frequency of events rather than their severity. **Small improvements of everyday performance may be more important than large improvements of rare performance.**
## Two types of safety management

<table>
<thead>
<tr>
<th>SAFETY-I</th>
<th>SAFETY-II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zero accidents</strong> – elimination of preventable harm</td>
<td><strong>GOALS / TARGETS:</strong> What is the goal or target?</td>
</tr>
<tr>
<td><strong>Counting adverse outcomes</strong> – things that go wrong.</td>
<td><strong>POSITION:</strong> Where are we now?</td>
</tr>
<tr>
<td><strong>Linear thinking:</strong> eliminate, prevent, protect</td>
<td><strong>MEANS:</strong> How can we improve?</td>
</tr>
<tr>
<td><strong>Work-as-imagined:</strong> WAI-WAD compliance</td>
<td><strong>FOCUS:</strong> What should be in focus?</td>
</tr>
</tbody>
</table>

**SAFETY-II**

- As much as possible goes well (AHARP)
- Measuring processes and functions – things that go well.
- Non-linear thinking: Improve, support, facilitate
- Work-as-done: Reconcile WAI-WAD
The bottom line

Few things go wrong, most things go well. Things can go wrong in more ways than we can imagine - and they are different. Prevention and protection are difficult to prove in practice.

Things usually go well in a limited number of ways - and they are similar. It is easier to learn from what goes well than from what goes wrong. Improvements can rather easily be verified and adjusted.
Thank you for your attention

Any questions?