Second stories:

working towards understanding resilience by understanding the deep structure of ordinary work

Presentation for
Conference on Studying Ordinary Work

EUROCONTROL
Barcelona, Spain, October 6, 2015

Richard I. Cook, MD
ricookmd at gmail dot com

Research Scientist
Department of Integrated Systems Engineering
Clinical Professor
Department of Anesthesiology
The Ohio State University
Columbus, OH 43210, USA

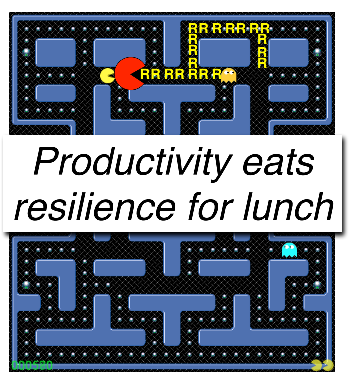
Emeritus Professor
Healthcare Systems Safety
Kungliga Tekniska Högskolan
Huddinge, SWEDEN

Conclusions — the setup BLUF [Bottom Line Up Front]

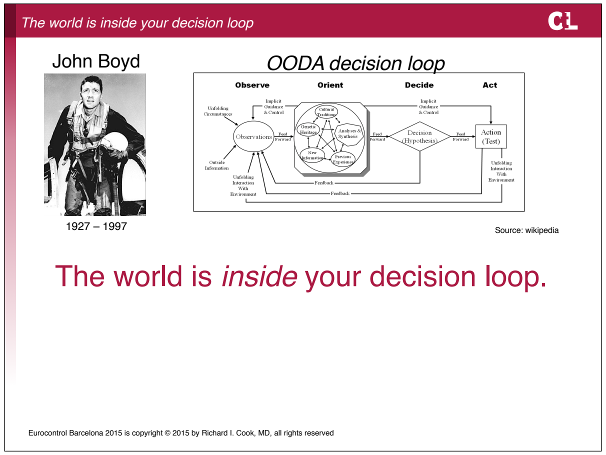
1. You have a resilient system.
2. The sources of resilience aren't clear.
3. The resilience is being eaten up as productivity
4. This is normal.
5. The problem is the low rate of accidents.
6. Nature will fix this problem for you.

Commercial air transportation is, in most of the world, extremely safe. This preconditions for this safety are the result of innumerable acts and decisions across the entire spectrum of the system. The system is exceptionally resilient but the sources of this resilience are not easy to see. Production pressure is consuming this resilience but the effects of this are hard to detect because the accident rate is currently very low. This complex, adaptive system will emit new accidents as resilience is eroded. This is a natural consequence and of the way that such systems work.

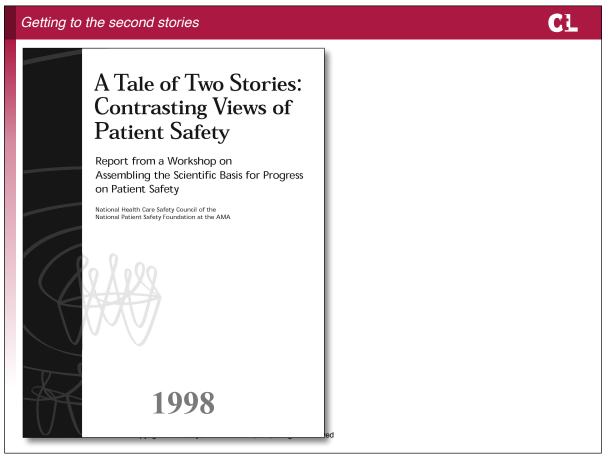
The basic problem is this: productivity eats resilience for lunch.



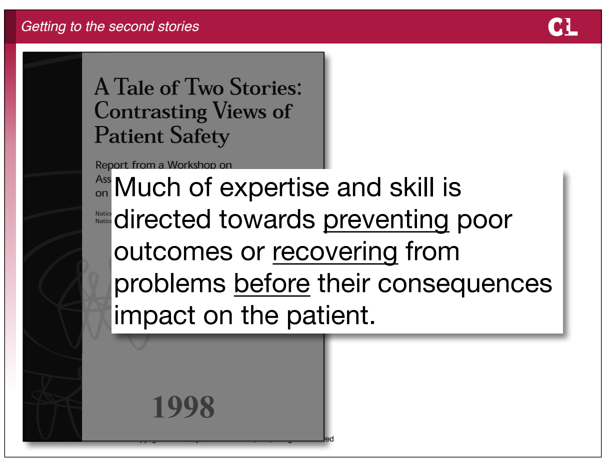
The relationship between productivity and resilience is a bit like a game of Pacman: productivity eats resilience until it runs into an accident.



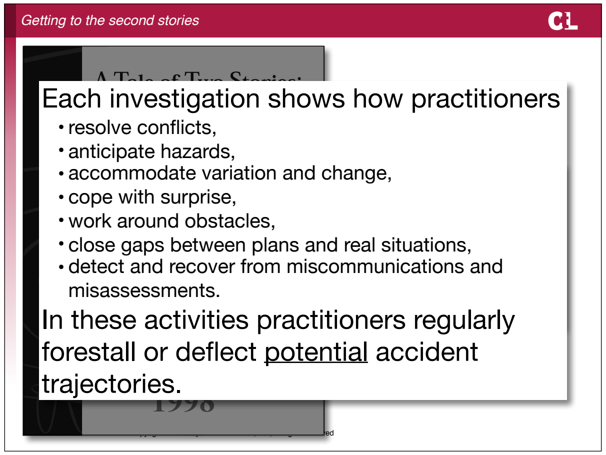
John Boyd coined the OODA decision loop: observe, orient, decide, act. In this model, if the situation changes faster than the loop time, decision making breaks down. Military operations seek to "get inside the either guy's decision loop" to make the enemy's decision making ineffective. In a larger sense, the world's rate of change is so fast that organizational decision making is unable to keep up. This is obviously true in ATM, where organizational and technical innovation is comparatively slow.



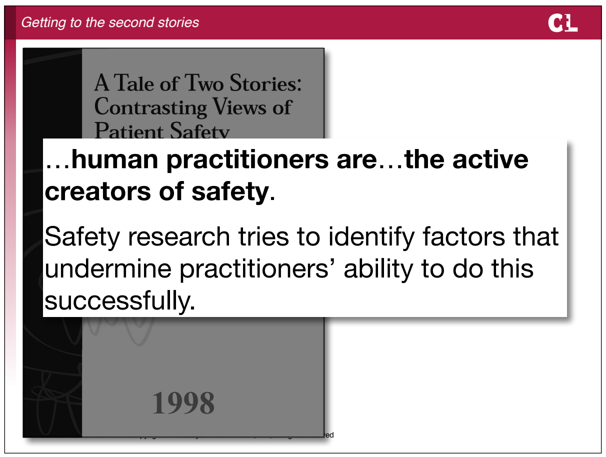
The idea of "second stories" is that looking narrowly at failure obscures the complexity, conflicts, and uncertainty of ordinary work. "A Tale of Two Stories" examines this closely and describes what is needed to make progress on safety. Second stories are about how people work and usually succeed in managing the conflicts and competing demands of everyday work. The idea of examining ordinary work more closely later becomes what Hollnagel calls Safety 2.



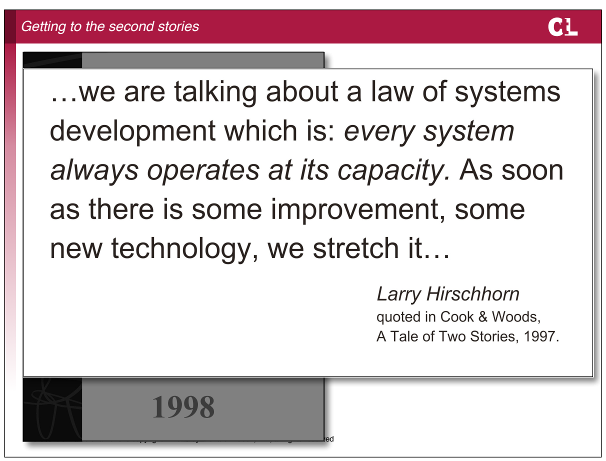
Sharp end work in hazardous work domains seeks to manage the processes to produce good outcomes. The role of operators in these domains includes supervising production and also detecting and responding when the process begins to fail. Recovering the process is a critical skill. Recovery is often only possible through sacrifice of one or more goals. The smooth escalation of sacrifice to preserve higher value goals is a hallmark of expertise.



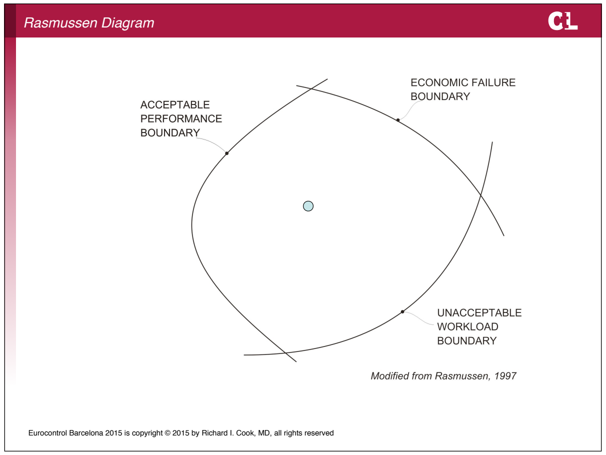
Specifically, explorations of second stories reveal how practitioners manage uncertainty. The deep knowledge of the processes, the values of different outcomes, and the limited-time opportunities available to deflect undesirable outcomes contribute to this work.



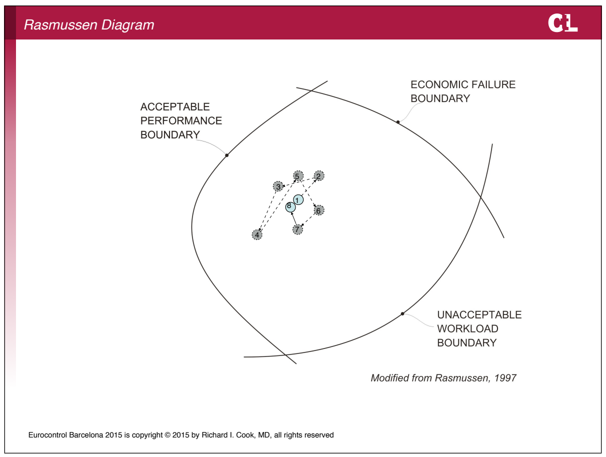
Rather than being inherently or intrinsically safe, over and over again we find that human expert practitioners create safety in order to manage the conflicting goals of operations. Safety research seeks to understand this work.



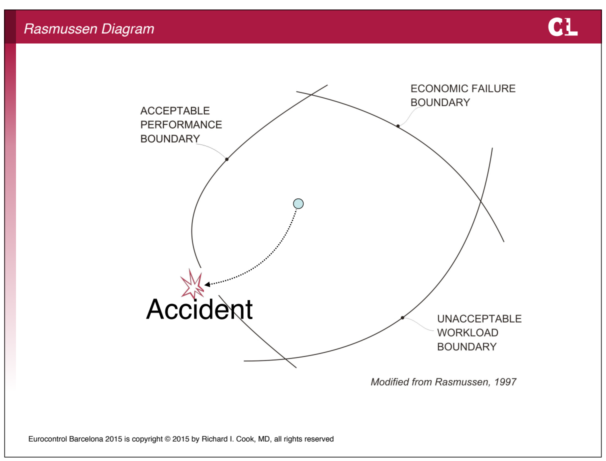
New knowledge and technology provide opportunities for change. Continuous economic and workload pressures lead us to exploit these opportunities. For example, we routinely operate on people today who would have been too old or too sick to undergo operations 20 years ago.



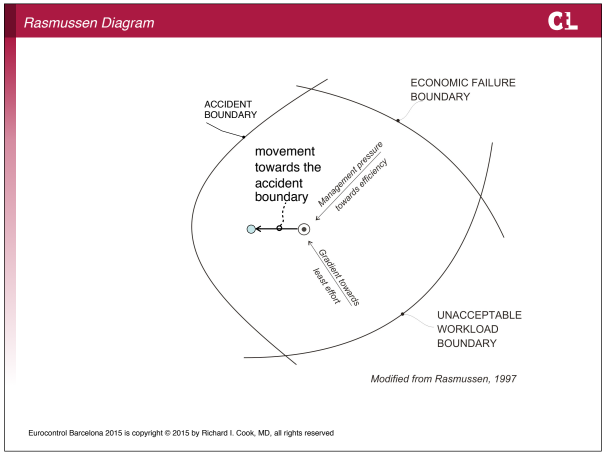
Rasmussen's system model has three boundaries: (1) an economic failure boundary, (2) an unacceptable workload boundary, and (3) an acceptable performance boundary. Crossing the economic failure boundary causes the system to halt because it is not viable, e.g. the company has gone out of business, the lights are off, the building is empty. Crossing the unacceptable workload boundary causes the system to halt because it no longer has exhausted its workers, e.g. people have collapsed and cannot function. Crossing the acceptable performance boundary leads to the system failing its purpose. At any moment, the system can be thought of as having a single operating point. If the system is functioning normally, the operating



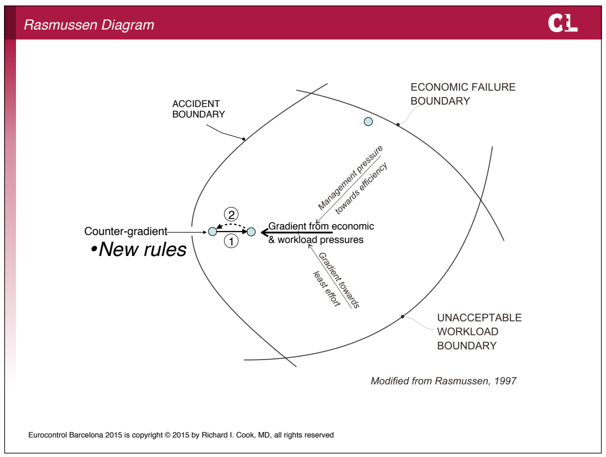
The operating point is constantly moving. The world is dynamic and things change all the time. The operating point is shifts with these changes. Most of these shifts are small and the pattern mostly moves the point in a local region.



Crossing the acceptable performance boundary generates an accident. The boundary labeled by Rasmussen as "acceptable performance boundary" may be relabeled as "Accident boundary".

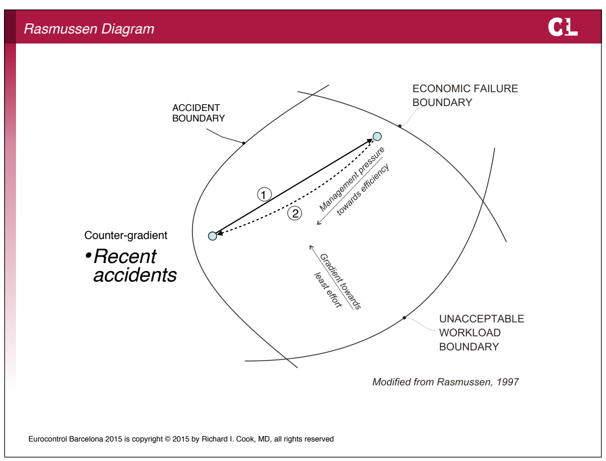


The closer the operating point gets to the economic and workload boundary, the greater is the pressure to move away from that boundary. This results in <u>gradients</u> of pressure. The combined effect of these gradients is to cause the operating point to slip (some people use the word “migrate”) towards the accident boundary.

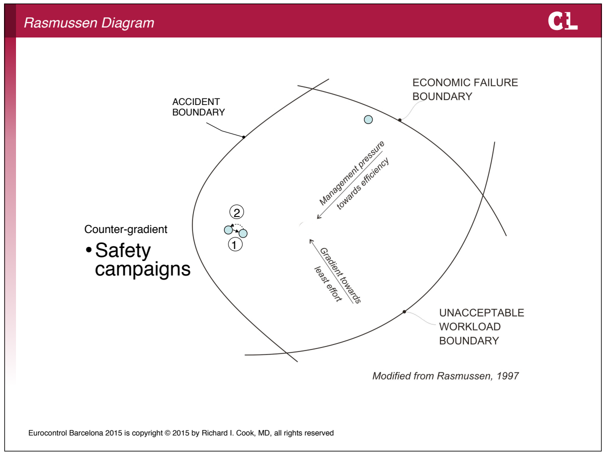


It is possible to counteract the gradient towards accidents. For example, (1) new rules can push the operating point up the economic and workload gradients and away from the accident boundary. But the economic and workload gradients are mostly fixed while the impact of rules is short term so (2) the operating point tends to resume its leftward movement. The effect of new rules is

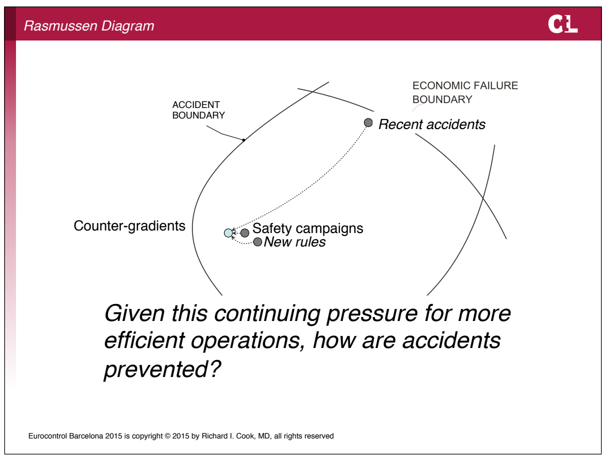
---



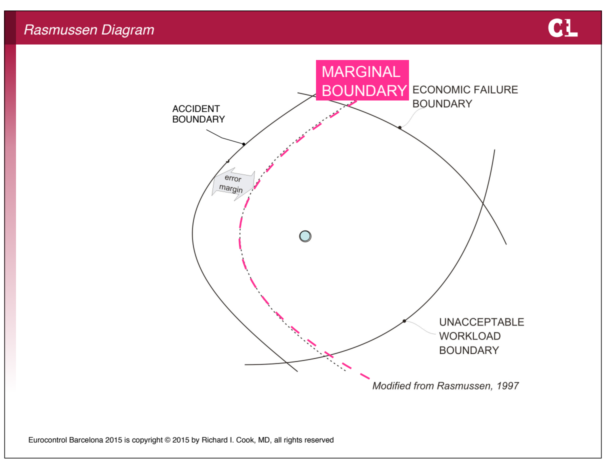
The effect of accidents can be profound, moving the operating point a great distance away from the accident boundary. But this effect also wanes with time as the accident experience recedes into the past. Ironically, the late effect of an accident may be to increase the economic gradient as the organization attempts to make up for the associated losses.



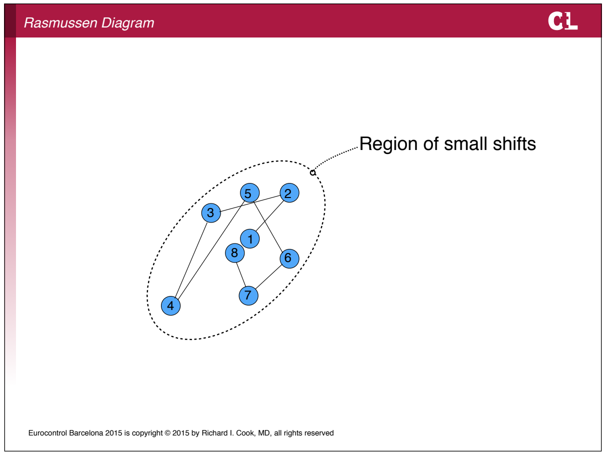
Safety campaigns by management have little effect on the operating point's location and that effect quickly dissipates. Examples of safety campaigns are the use of slogans, publications, and posters encouraging safe work or increased attention to safety. Such campaigns are undertaken mainly to give the impression that the organization values safety. The real conflict between these claims and



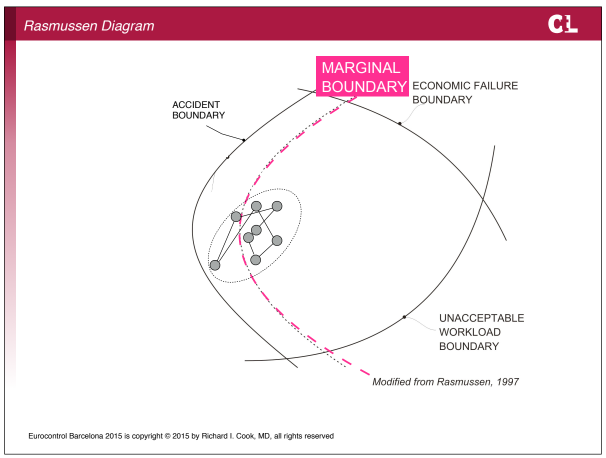
The key idea here is that all the available counter gradients are temporary while the economic and workload gradients are permanent. The effect of introducing a counter gradient — even a rather profound one such as a recent accident — tends to fade over time. If the economic and workload gradients remain the same the result will be that the operating point will continue to migrate



The goal of avoiding accidents leads to establishment of an organizational boundary some distance from the accident boundary. This is sometimes called the "error boundary" or, sometimes, safety margin, but a better name is marginal boundary. The premise of the marginal boundary is that deliberately restraining the operating point within this boundary will prevent accidents.

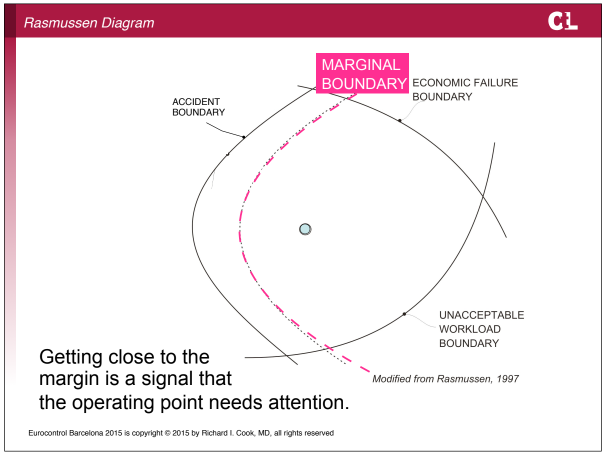


Recall that the operating point is constantly shifting its location over time (range: seconds to days or even weeks). On average, these shifts cancel out over time. Tracking these shifts produces a region for the operating point movement.

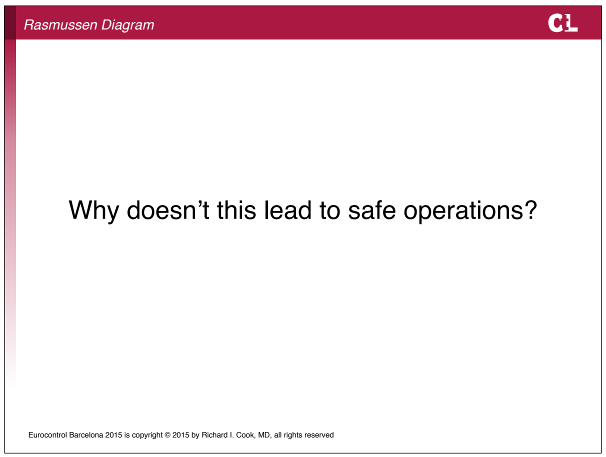


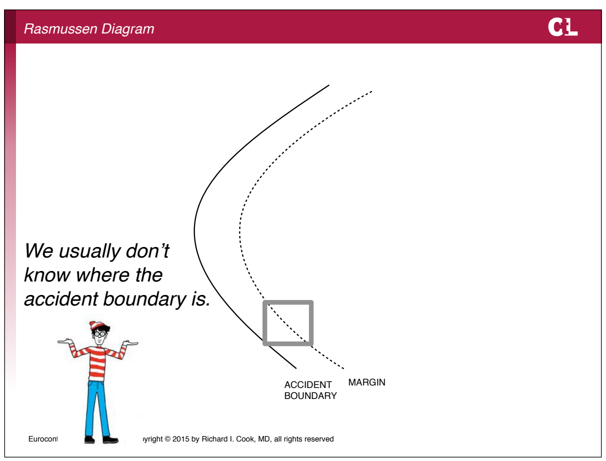
The marginal boundary is placed far enough away from the accident boundary that the operating point small shifts are unlikely to generate an accident.

Overall, the constant gradients from the other boundaries push the operating point towards the margin. This leads us to state a general rule that the operating point will remain near the margin.

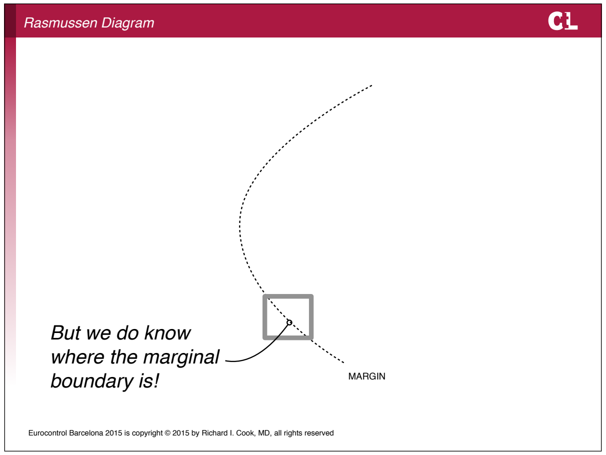


The marginal boundary is a composite of the rules, understandings, professional conclusions, and worked out details about what is acceptable. The marginal boundary is specific, mundane, practical. It is usually well understood, at least locally, within the organization. It is the reference for the operational day-to-day. It is socially defined — although it involves so much technical understanding and rationale that it is more proper to describe it as 'socio-technical'. The boundary is intended to keep the operating point far enough away from the accident boundary that, in ordinary circumstances, no accidents should occur.

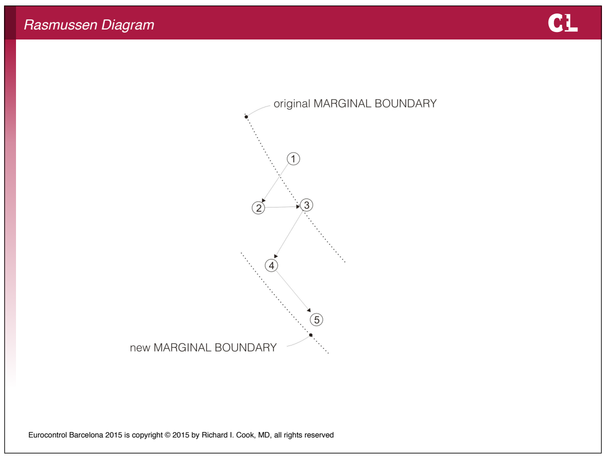




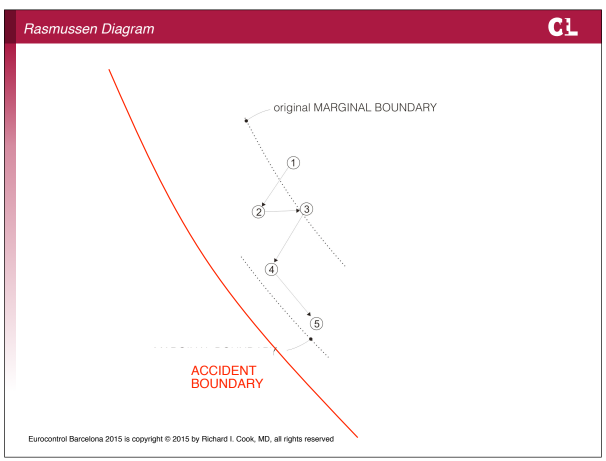
When the accident rate is low, there is little information available about the location of the accident boundary.



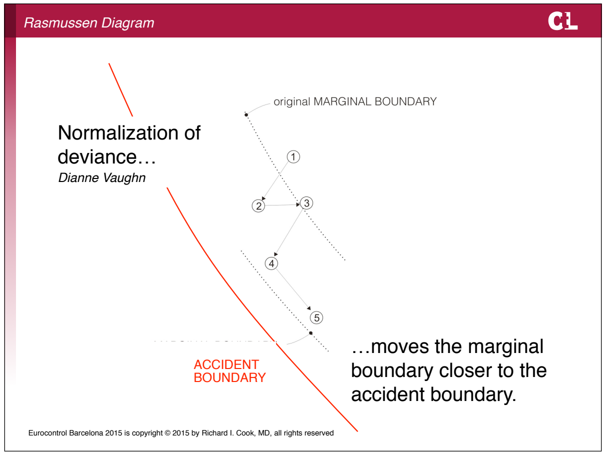
In contrast, the location of the marginal boundary is usually widely known and well appreciated. In the next slide we will blow up the figure to concentrate on the situation inside the box.



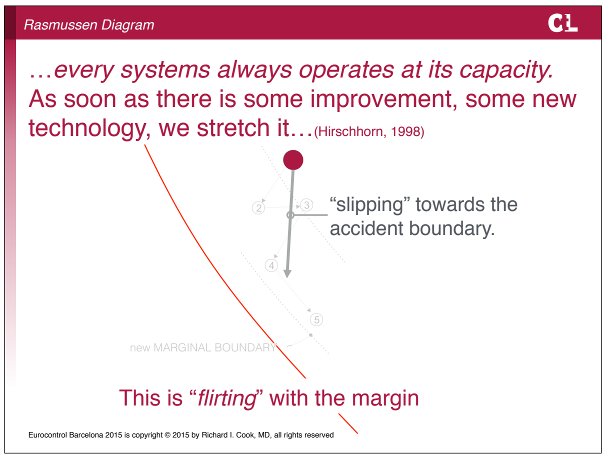
Ordinary operations will cause the operating point to cross the marginal boundary (1 to 2). This routinely leads to efforts to push the operating point back across the boundary (2 to 3). Repeating the experience may lead people to conclude that there is no real hazard associated with being in this over-but-still-near-the-boundary area (3 to 4). It is then possible to conclude that the marginal boundary is too conservative and that operations can safely be conducted in this region (4 to 5). This leads the marginal boundary to be revised outwards.



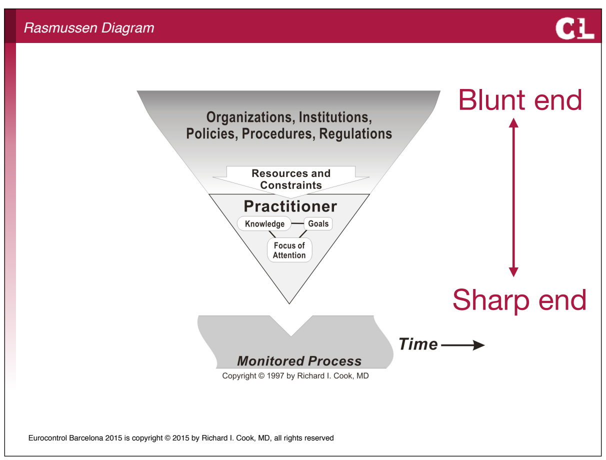
But if the accident boundary has not changed its location, the result of shifting the margin outwards is to allow “normal” operations to be conducted nearer the accident boundary. Now the everyday movements of the operating point that sometimes lead to crossing the marginal boundary are much more hazardous. Recall that the accident boundary location is not known precisely when accidents are rare. For this reason, this adjusting of the margin may repeat and until operations are allowed very near the accident boundary.



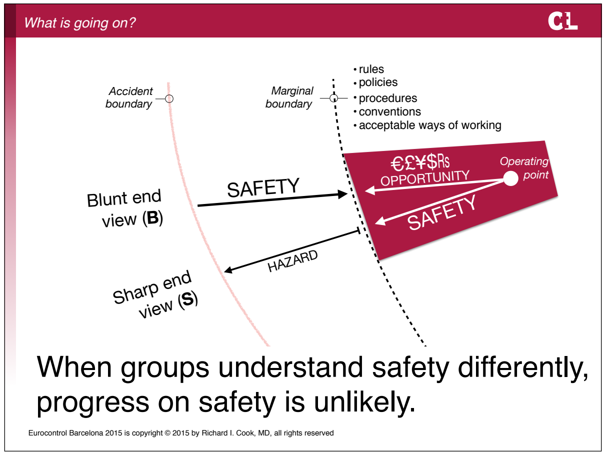
This is one way of interpreting what the sociologist Dianne Vaughn has called "normalization of deviance" in systems terms. [NB: "deviance" is a technical term with quite specific meaning in sociology. The author does not agree that the shuttle Challenger accident is an example, as Vaughn asserts.]



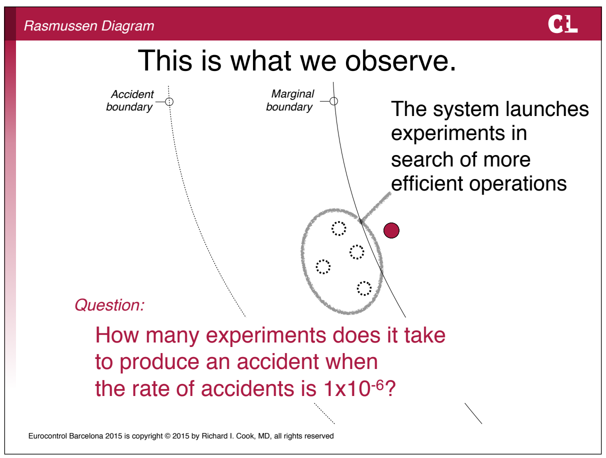
Overall, the impact is that the operating point 'slips' towards the accident boundary. This is especially a problem in "safe" systems, i.e. systems where the accident rate is very low, because there is little contemporaneous information about where the accident boundary actually is!



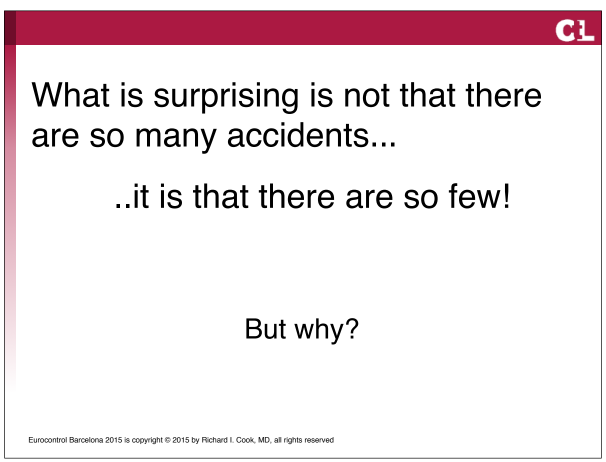
What is safety? The answer depend on who is answering the question. Managers and administrators working at the blunt end of the system may answer quite differently than practitioners working at the sharp end.



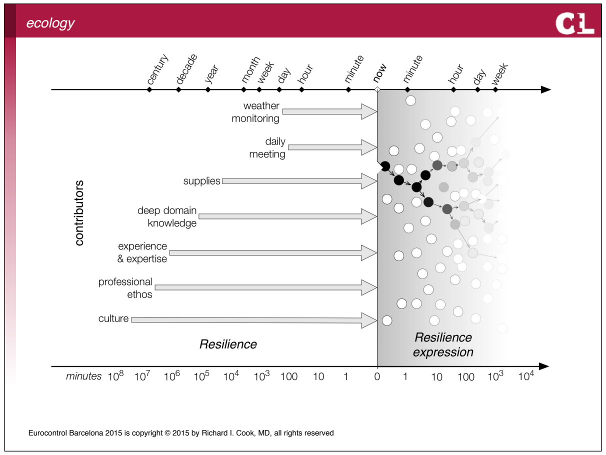
The blunt end view of safety is that it is what is provided by the marginal boundary. Blunt enders put great emphasis on the rules, processes, and procedures that delimit the marginal boundary. When the operating point is inside the marginal boundary, the distance to the boundary represents unrealized economic an labor benefits. The distance is an opportunity. For the sharp enders, this distance is safety. Although its movements are usually small, there are situations where the operating point can move in large steps so keeping it far away from the marginal boundary contributes to safety. Managing this conflict is an organizational priority.



One way to think of safety in a low-accident-rate system is that the system is constantly launching operational safety experiments. These are efforts to improve the efficiency of the system operations while avoiding accidents. Exploring the boundary of safety is seen in virtually all such systems, although most experiments are not described as such! Especially when the accident rate is very low, experiments may produce positive (i.e. no accident) results for a long time. Especially when the accident boundary is being changed (e.g. by introducing new technology) this may be the only way in which the payoffs for such improvements can be obtained. Again, recall Hirschhorn: "...every systems always operates at its capacity. As soon



This presentation should prompt the viewer to ask, "Why then do we not have many accidents?"



One answer to this question is that the system is highly resilient rather than highly reliable. Resilience is the capacity to respond to a disturbance, to shift performance so as to achieve higher level goals, and to return to “normal” operations afterwards. When examining the micro level we find an ongoing interplay between the situational demands, the array of hazards that threaten, and the actions of practitioners. Instead of being a steady-state, static, “locked down” environment, complex adaptive systems function in an uncertain, rapidly changing world.

Les Liaisons dangereuses

*But how? (this is the **big** research question in safety)*

What operational tactics do we observe?

- Flexibility in resource assignments (load following)
- Dynamic restructuring of task work
- Deliberate tradeoffs (e.g. explicit goal sacrifices)
- Reactive measures

What should be the strategic approach?

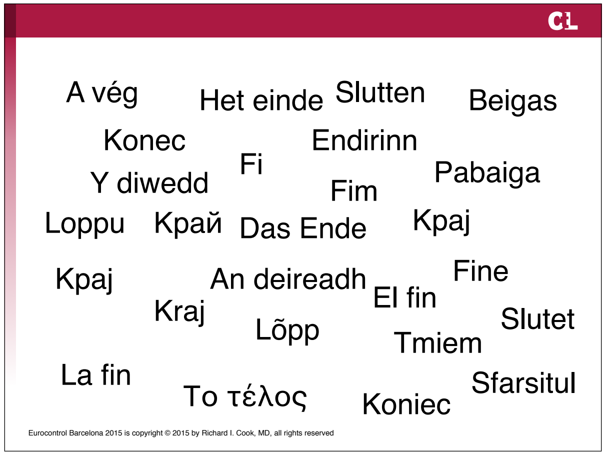
- Second story inquiry (e.g. study sector splitting & other decoupling methods)
- Looking at recovery
- Better anticipation help (e.g. vizualization tools)

What is resilience in ATM? This is the big research question we are trying now to explore. The most important “given” in this exploration is that the ATM system is already resilient and our research should discover how that resilience plays out in daily work. Some operational tactics are already identified: load following processes are common and depend on anticipating near and far term requirements; task work itself can be restructured on the fly to accommodate sudden changes; practitioners (controllers and supervisors) sacrifice some goals to maintain opportunities to respond, e.g. briefly delaying departures to manage traffic crushes; the system can react quite deliberately to major disturbances (e.g. weather). The exploration of these sorts of activities is expected to make the resilience of the ATM system clear and set the stage for open discussions of how that resilience is to be sustained.

Conclusions

1. There will be more accidents.
2. You are already doing safety 2.
3. We are trying to understand how you do it.
4. We know that it is hard work.
5. We understand the world is changing fast.
6. The system is already adaptive.
7. We think you will be successful in coping.
8. We offer this ‘stuff’ as a language of safety.

Thank you for your kind attention!


A vég
Het einde
Slutten
Beigas
Konec
Endirinn
Fi
Y diwedd
Pabaiga
Fim
Loppu
Край
Das Ende
Kpaj
Kpaj
An deireadh
Fine
El fin
Kraj
Slutet
Lõpp
Tmiem
La fin
Sfarsitul
Το τέλος
Koniec
Eurocontrol Barcelona 2015 is copyright © 2015 by Richard I. Cook, MD, all rights reserved