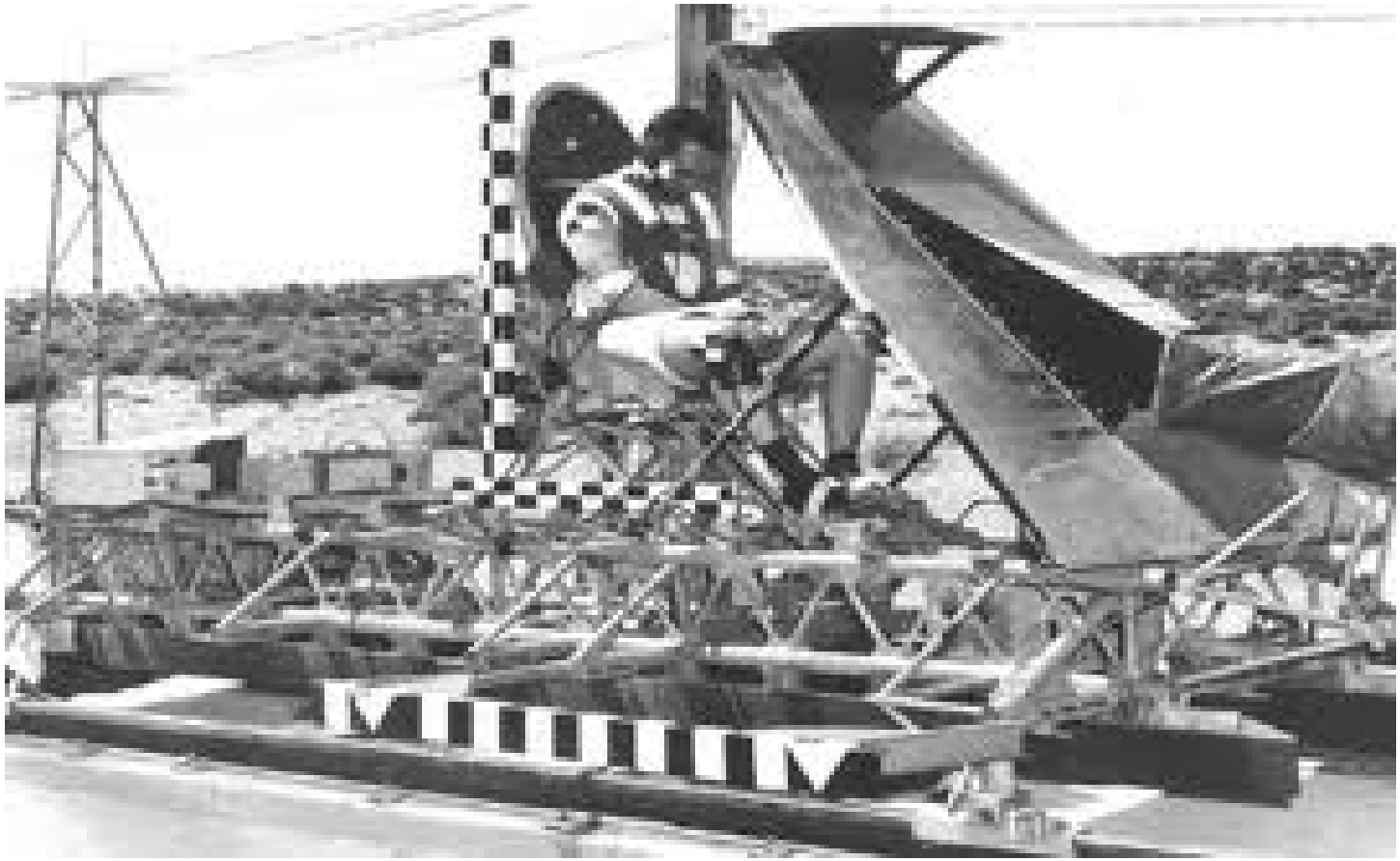
The Relationship between Safety and Security

Pat Baird
pat.baird@philips.com
May 18, 2017

innovation + you

PHILIPS

Risk Management = Managing Murphy's Law



PHILIPS

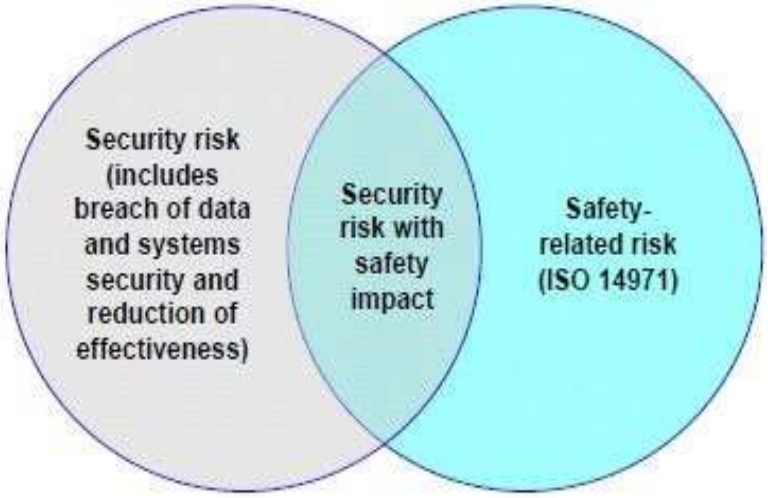
Similarities between Safety and Security

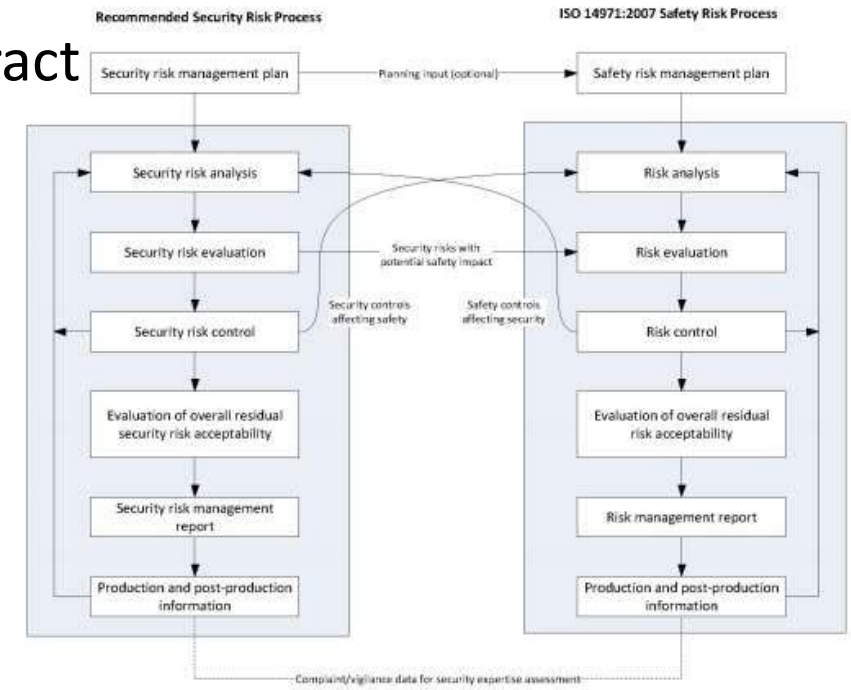
1. Similar definitions of HARM:

14971 “Physical injury or damage to the health of people, or damage to property or the environment”

80001-1 & TIR57 “Physical injury or damage to the health of people, or damage to property or the environment, or reduction in EFFECTIVENESS, or breach of DATA AND SYSTEM SECURITY”

2. Safety & Security overlap and interact





Source: AAMI TIR57:2016 Principles for medical device security – Risk management

PHILIPS

Risk Management, In a Nutshell

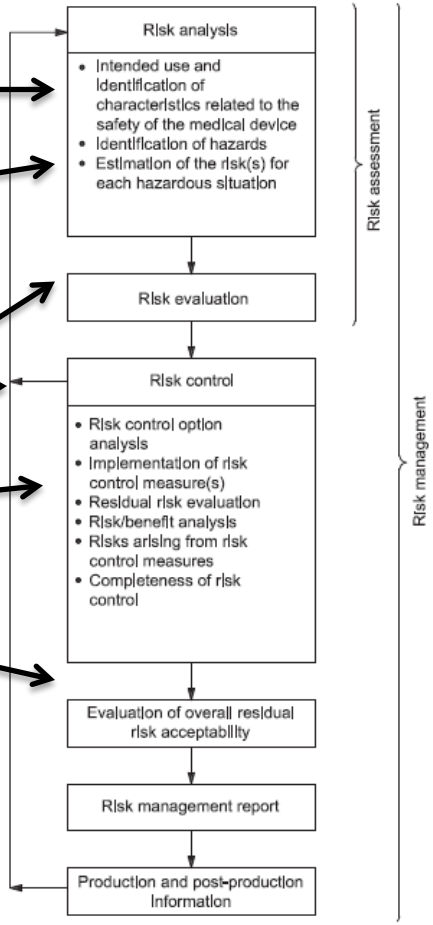
Risk Management can be summarized as 4 questions, regardless of if we are talking about financial risk, safety risk, security risk, etc.

1. What are you trying to do?
2. What can go wrong?
3. What are you doing to do about it?
4. Did it work?

PHILIPS

How does this map to 14971 ?

1. What are you trying to do?
2. What can go wrong?
3. What are you going to do about it?
4. Did it work?



PHILIPS

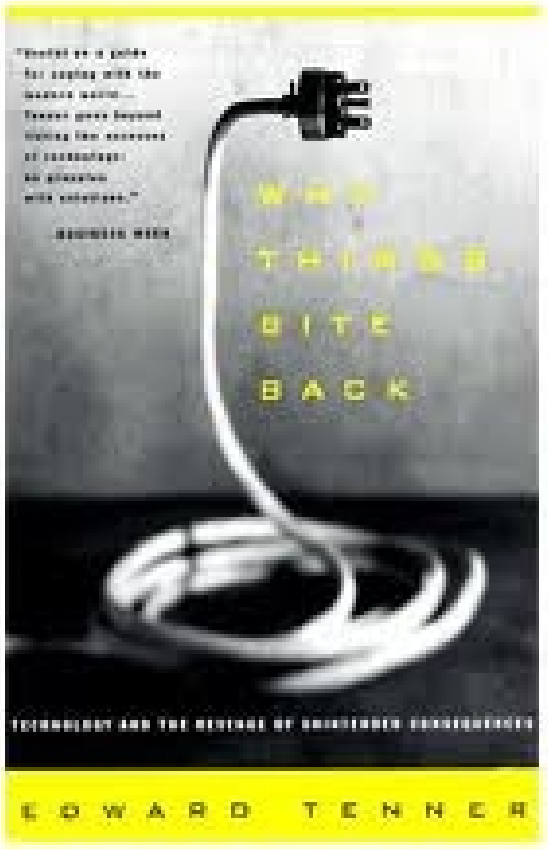
Similarity: Labeling Controls not as effective as other options

PHILIPS

Similarity: Unintended consequences

Attempts to mitigate sometimes results in even more dangerous behavior. We are required to consider the consequences of the mitigations.

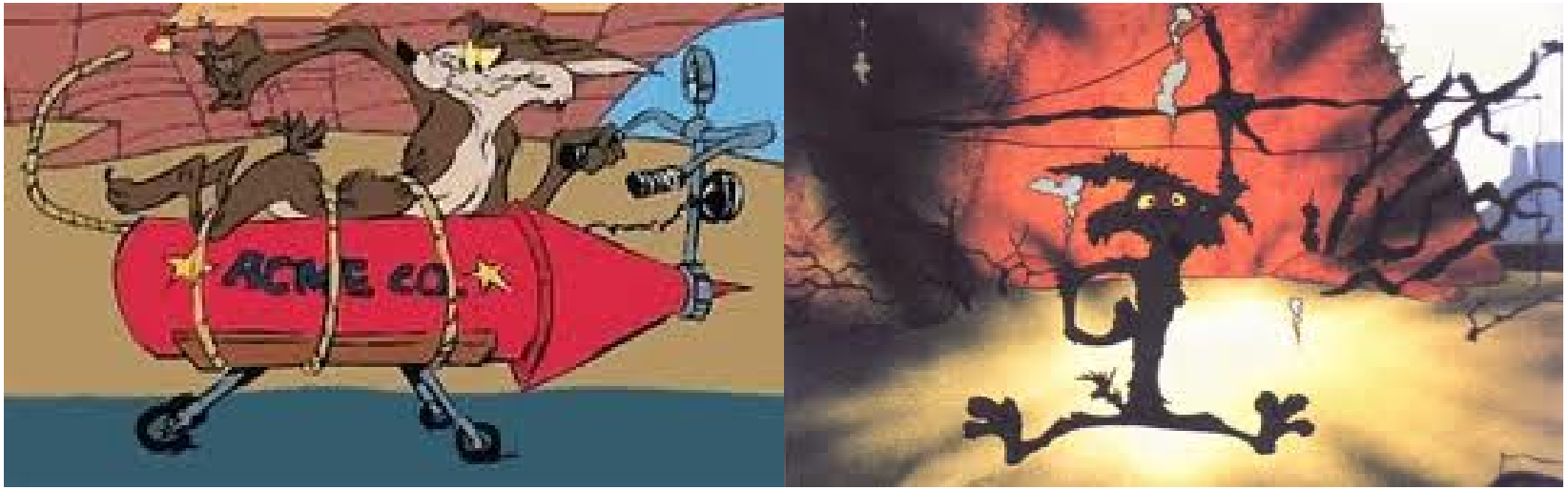
- Example 1: Weather radar for North Atlantic fishermen was intended to give them more time to leave a dangerous area
- Instead, the captain know exactly when a storm will arrive, and stays until the last minute
- Example 2: When anti-lock brake systems were first introduced, the number of car crashes in the US declined.
- However, once ABS was the norm, the number of crashes resumed it's previous level. Why?
- People started pressing on the brake pedal later; sometimes not giving themselves enough time to stop.



Why Things Bite Back, Edward Tenner

PHILIPS

Similarity: Software Of Unknown Provenance (SOUP) & Commercial Off The Shelf Software (COTS)



- Just like other domains, software needs to pay attention to supplier quality.
- You need to make sure that any software components that you use in your product actually work, but you often don't have access to the design documentation nor source code.

PHILIPS

Expectations for SOUP & COTS

A common questions is how SOUP fits into risk management activities.

The manufacturer of the final product is responsible for identifying how SOUP impacts safety and security, and is responsible for evaluating and taking action when necessary.

Remember the 4 Steps:

1. What is the SOUP trying to do?
2. What can go wrong?
3. What are you doing about it?
4. Did it work?

PHILIPS

Similarity: Importance of Verification AND Validation

Need to verify / validate that the risk control was effective.

Shouldn't just verify that risk control has been implemented, make sure the risk control is effective.

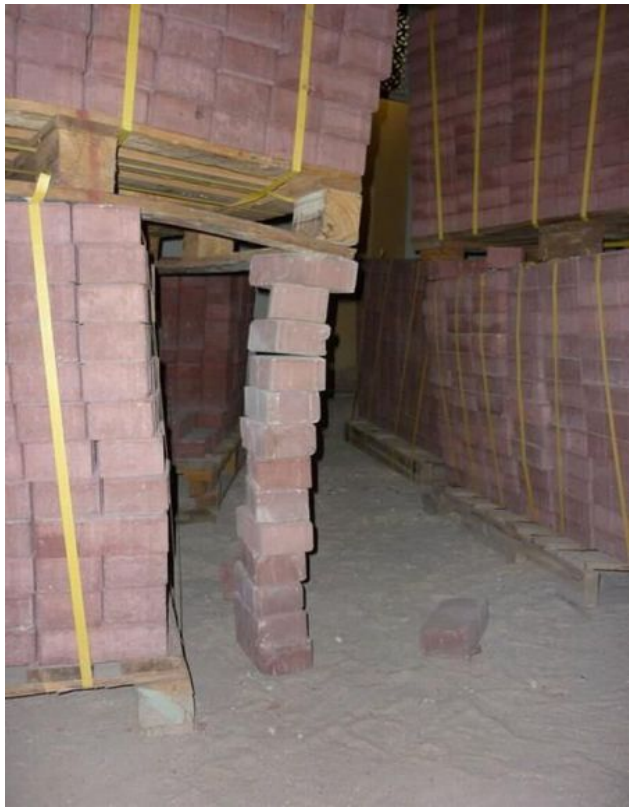
PHILIPS

Similarity: Event-based and periodic reviews

Need to continually monitor post-market events,

even near-miss,

as well as monitoring ongoing changes over time.



PHILIPS

Differences between Safety & Security

- Safety is about keeping the product from affecting the environment (stuff outside of the product)
- Security is about keeping the environment from affecting the product.

- Safety is making sure the product does what it is supposed to do
- Security is making sure it still does what it should despite external threats

PHILIPS

Differences in Security Risk Evaluation

“Risk = Probability x Severity”

Probability for **Safety** Risk Management is a function of design – material selection, tolerances, design margin, and a function of manufacturing – Cpk, etc. Things that are easily estimated.

Probability for ***Security*** Risk Management is a function of motivation – financial gain, mayhem, and a function of opportunity – open vulnerabilities, etc. These things are not easily estimated or even known.

Probability for **Safety** Risk Management largely stays the same over time, and only change as the design or manufacturing changes.

Probability for ***Security*** Risk Management can immediately change from “Remote” to “Every Time” once an exploit is published on the internet.

PHILIPS

Differences in Risk Evaluation

"Risk = Probability x Severity"

Severity of Harm for **Safety** Risk Management is substantially driven by the intended use. **Severity** is driven by what you are.

Severity of Harm for ***Security*** Risk Management can be completely unrelated to your product. **Severity** is driven by who you know.

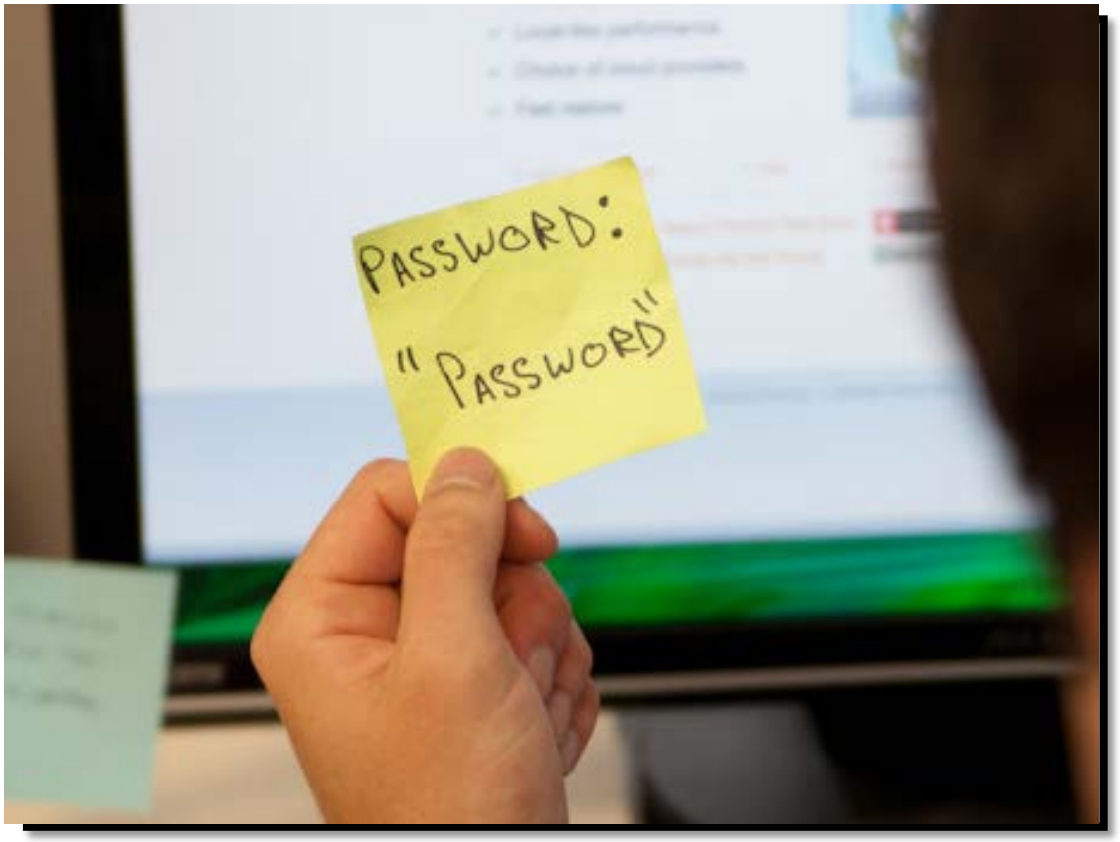
"Everything is a Target, Everything is a Weapon" [Control System Cyber Security How to Properly Protect and Maintain, I. Verhappen, S. Gold, CP 2013 Panel Discussion]

PHILIPS

Differences in Human Factors

In **Safety** Risk Management, a product that is easy to use is often safer to use.

In ***Security*** Risk Management, a product that is easy to use is often exploitable.



PHILIPS


PHILIPS