Our assumptions will very likely be wrong; the unexpected will probably occur

Michael Fisher

Department of Computer Science, University of Manchester, UK

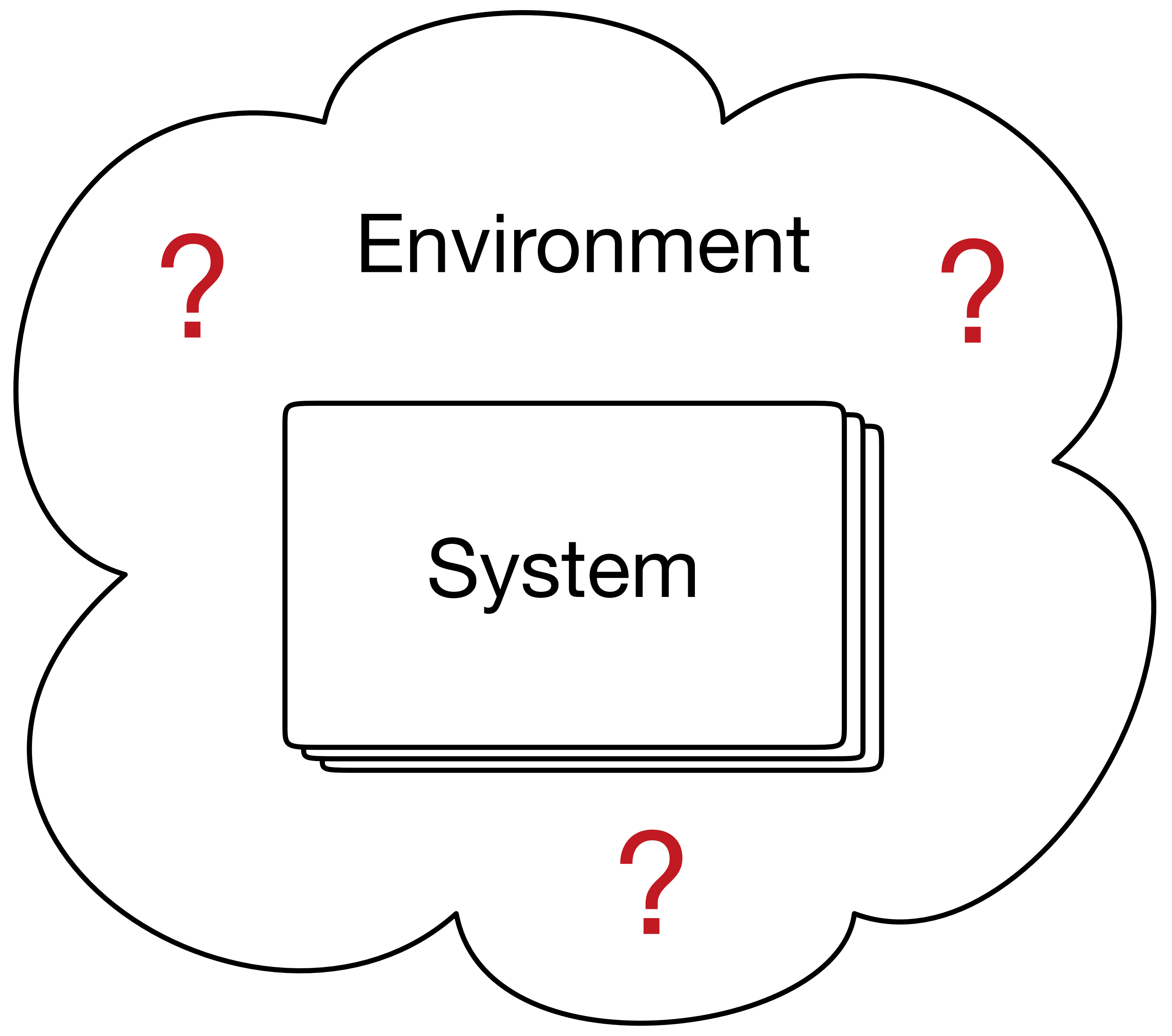
`https://web.cs.manchester.ac.uk/~michael`

October 2023, *IROS'23 Workshop: "It Works Really Well"*

It Works Very Well

The Specification of our systems can be very precise.

But what about the specification of the environment in which the system acts?



We might simplify/assume too much

1. sometimes to fit our tools/techniques
2. sometimes accidentally, through generous assumptions
3. sometimes deliberately, as we can’t describe the full extent of the environment

Need to be explicit about (and even formally capture) our assumptions

It Works Very Well

What it is we verify might also be (over) simplified.

A typical route to properties might be through some sort of hazard/risk analysis

But these are often/sometimes very conservative, just highlighting the obvious risks.
….. if everything is predictable then we can pre-plan the outcomes we want

Especially in *autonomous systems* we must be able to cope with the unexpected

Need to verify what our autonomous system will do when it meets the unforeseen
….. otherwise, what's the point of autonomy??

It Works Very Well

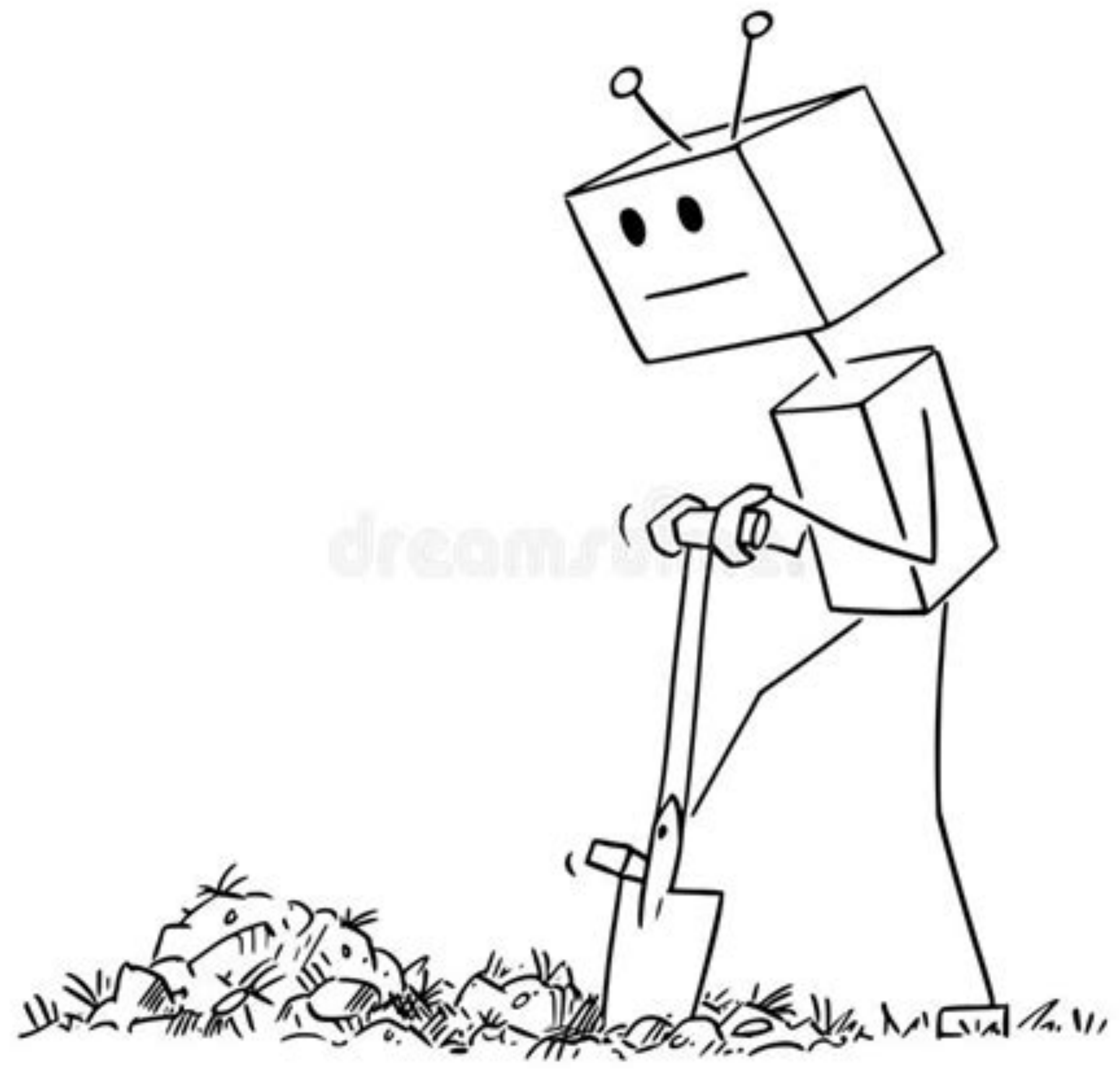
Yes/no verifications outcomes are relatively straightforward.

But:

"Robot will succeed in digging the hole 73% of the time"

What does this mean?

Have we simplified
- the *environment* - Physics of sand, for example?
- the *property* - abstraction of "digging", abstraction of "success"
- *time/statistics* - assumed uniformity based on observations?
- etc…



Especially with probabilistic outcomes, we must be very clear what is meant

“Our assumptions will very likely be wrong”

1. Be **explicit** with your assumptions, especially about the environment

2. Static verification will likely be based on these assumptions - make this **clear**

3. Use dynamic verification methods (e.g. RV) to **check** these assumptions at runtime

   In general, use multiple, distinct verification techniques to corroborate each other

4. Have some recovery/failsafe mechanism to cope when assumption **violation** occurs

“The unexpected will probably occur”

1. The unforeseen will occur - we need to verify what our autonomous system will do in such cases

2. Even though component failure is to be expected, we must verify the recovery mechanisms thoroughly.

3. And, importantly, how any failure impacts on the assumptions we had for other verifications!