Functional Safety Discipline

SIL Slam
Safety & Availability



10 10 10 BY2020

Christian Demski

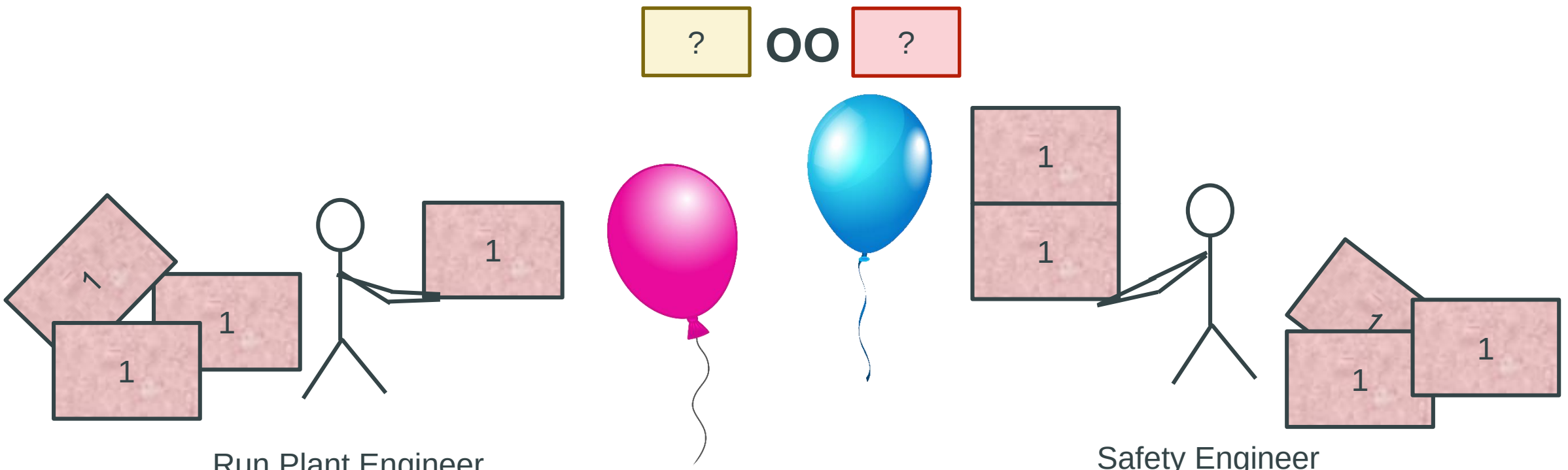
Technical Expertise and Support

Leverage Globally, Act Regionally, Execute Locally – ***Faster and Smarter***

This is the discussion we know.

Availability

Safety



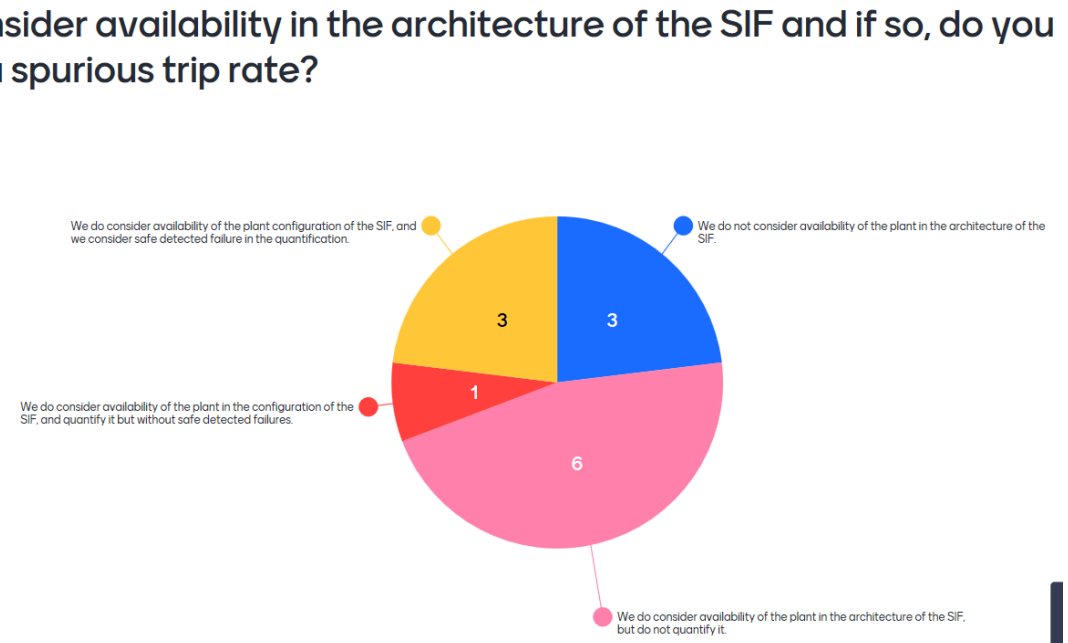
Run Plant Engineer
Reliability Engineer

Safety Engineer

Questions to the audience?

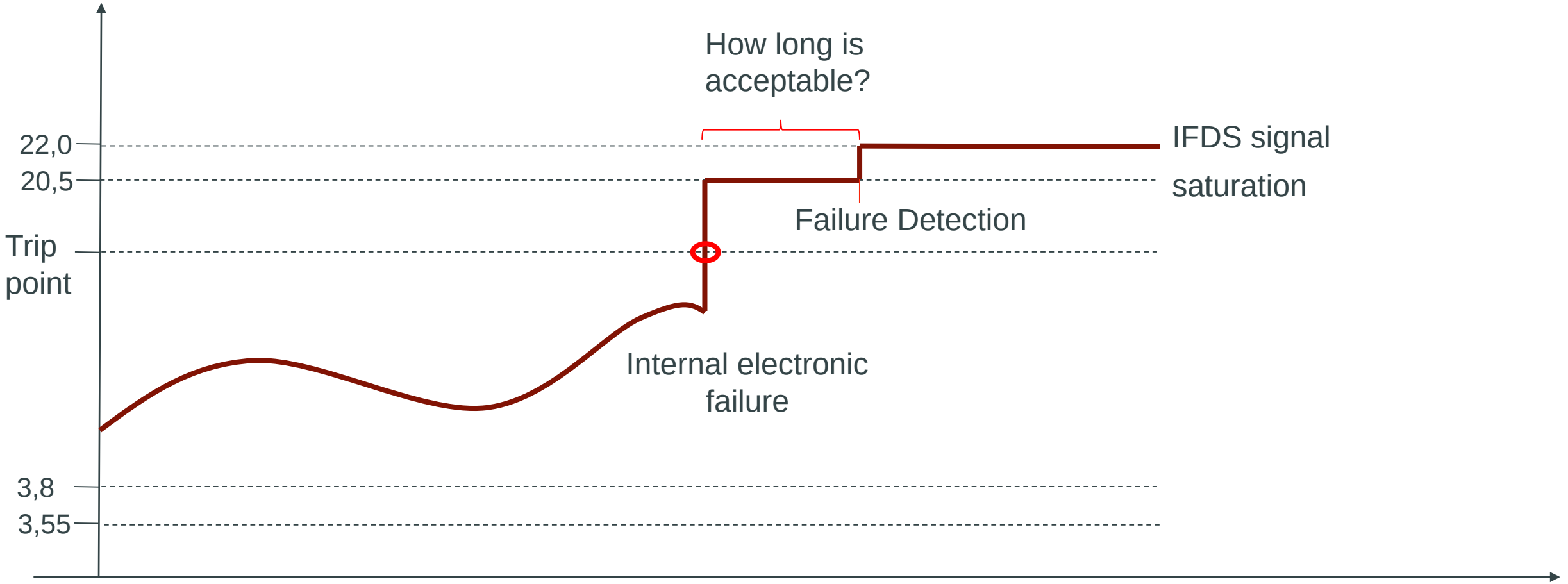
Do you consider availability in the architecture of the SIF and if so, do you calculate a spurious trip rate?

- We do not consider availability of the plant in the architecture of the SIF.
- We do consider availability of the plant in the architecture of the SIF, but do not quantify it.
- We do consider availability of the plant in the configuration of the SIF, and quantify it but without “safe detected” failures.
- We do consider availability of the plant configuration of the SIF, and we consider “safe detected” failure in the quantification.



Technical Expertise & Support
Leverage Globally
Act Regionally
Execute Locally
Faster and Smarter

An actual event in the plant lead to some thoughts…..

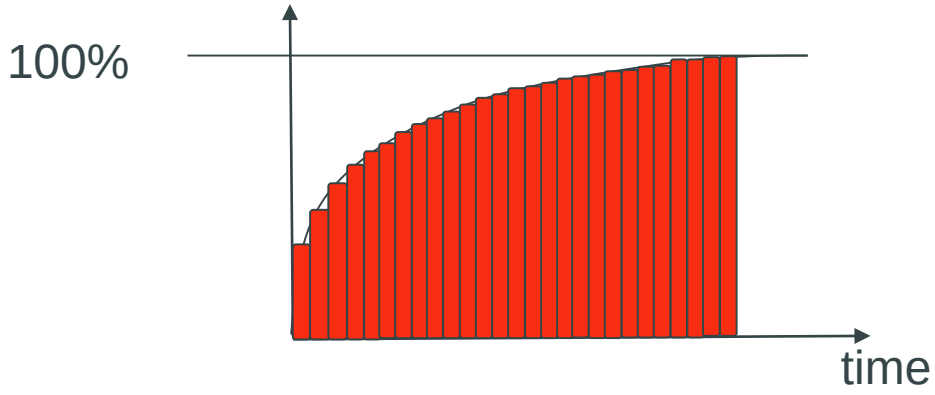


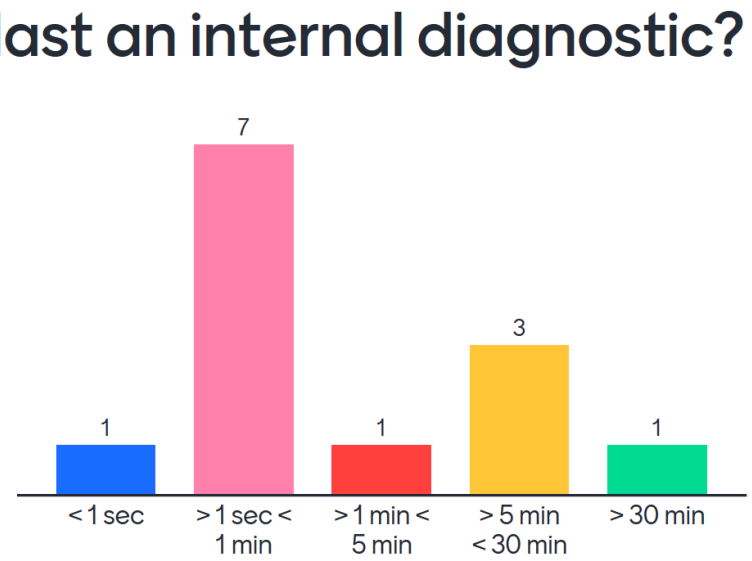
How long last an internal diagnostic.

- < 1 sec
- > 1 sec < 1 min
- > 1 min < 5 min
- > 5 min < 30 min
- > 30 min

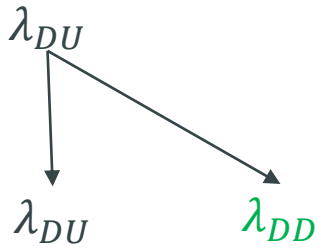
In most of the cases it takes more than 30 min…..

SUM (Number of failures * frequency of occurrence)





What is available outside of IFDS different modes of diagnostic



- **Hi/Lo:** This is programmed in the DCS to detect a shortcut or an open circuit
- **Diagnostics (fail safe):** is the internal diagnostic of the device that leads to the output signal in the area of the current indicting a failure (Namur < 3.6 mA or > 21.5 mA)
- **Intercomparison:** comparing the signals of devices against each other
- **Rate of change:** algorithm programmed in the DCS meant to detect changes in the signal that cannot happen under process condition indicating a failure of the device.

Questions we want to discuss in the “SIL Sprechstunde”?

- Do we have safe detected failures even as they do not occur in most certifications?
- What are the boundaries to claim safe detected failures?
- Does this also might have an impact on the dangerous failures or the safety integrity at all?
- How do different methods of diagnostic reveal those failures?
- How do different configurations impact the ability to use safe detected failures?

Thank you for the attention

Questions, comments, discussion points?

In case of any comment or want to have a later discussion and please contact me

Christian Demski
Dow Deutschland Anlagenge...
IEA SIS Expertise Area Leader
Technical Expertise & Support
+49 41469 13814 Work
Other
CDemski@dow.com
Postfach 1120
Stade, ND 21677

Technical Expertise & Support
Leverage Globally
Act Regionally
Execute Locally
Faster and Smarter