Common weaknesses observed in functional safety concepts

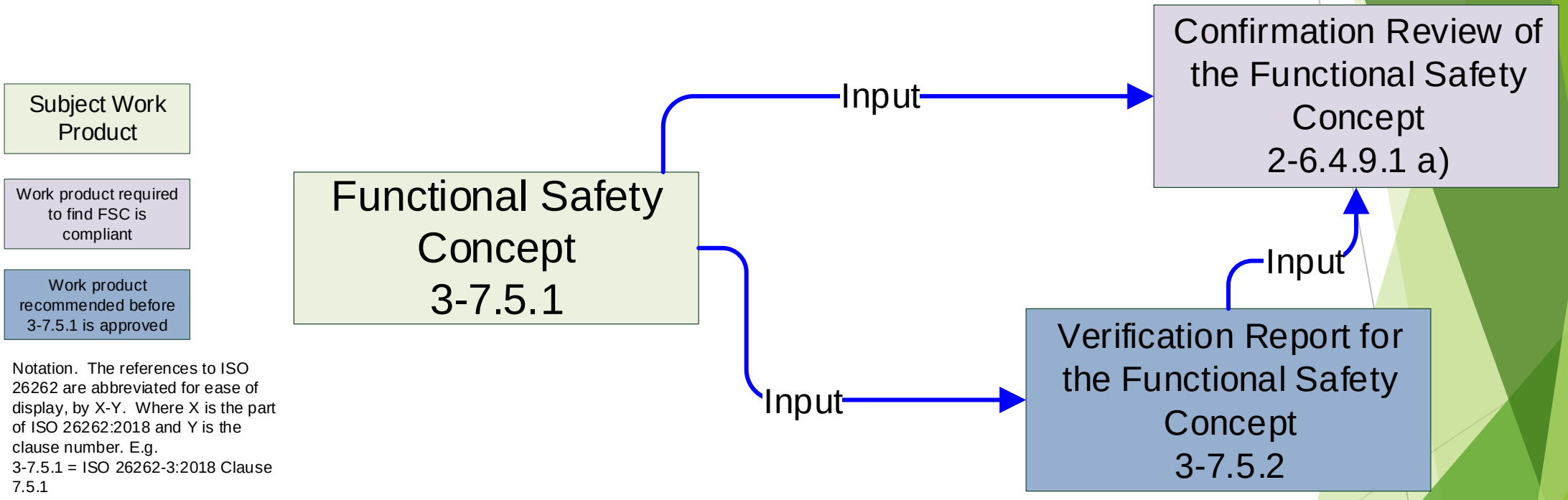
And How to Avoid Them

Presented by Mark Cousen

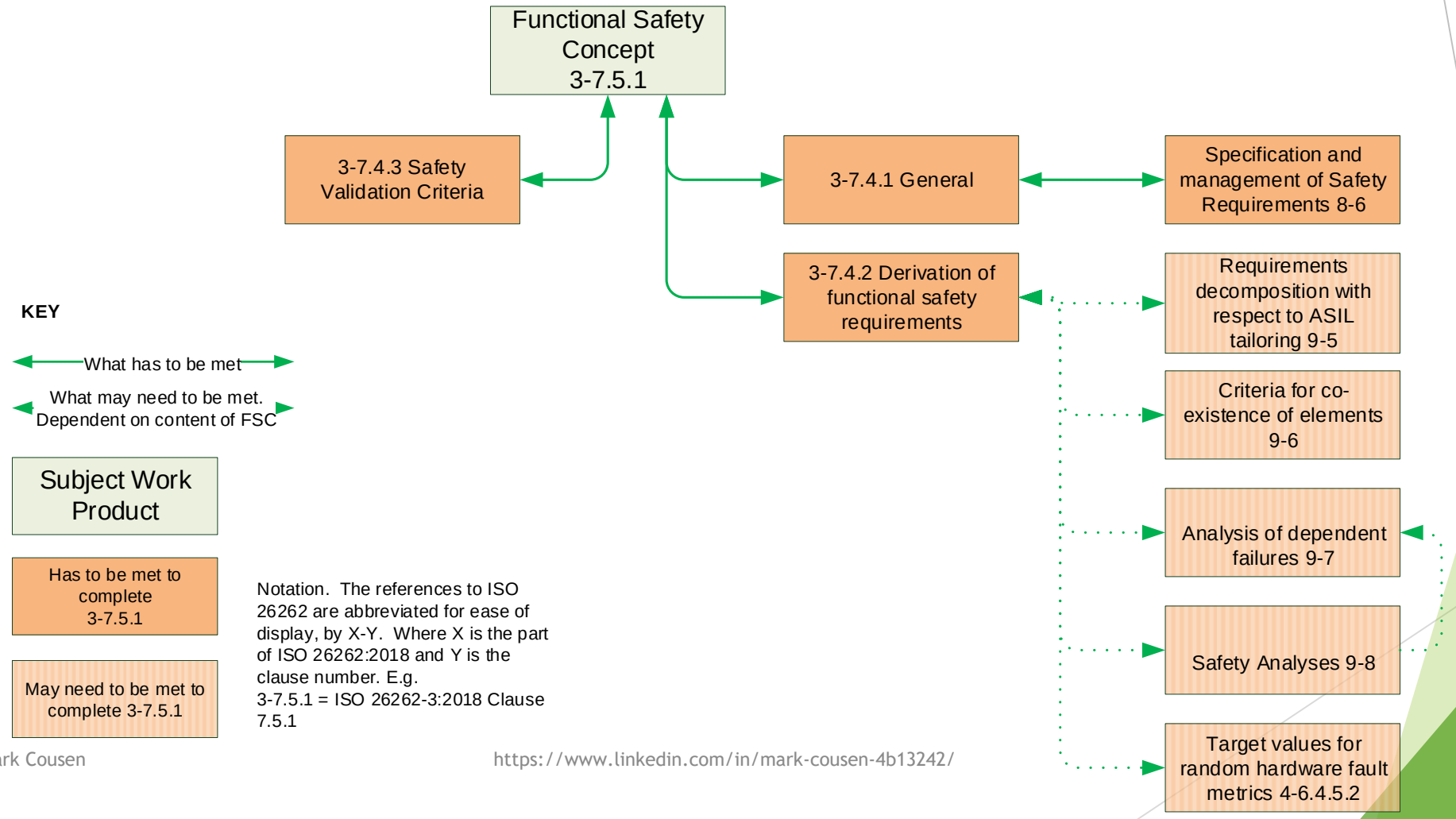
Agenda

- Presentation of observations and recommendations
  - What is required for an FSC
  - What are the weaknesses seen in application of ISO 26262 in the development of the FSC
  - What is the false assumption that is suggested to be the root cause of these weaknesses
  - Argumentation why this assumption is false and why it is the root cause
  - Proposed solution
- Discussion of the comments provided by participants. During the presentation provide comments on:
  - Are there any weaknesses not covered by the false assumptions that are proposed,
  - Are there any other false assumptions made that cause FSC weaknesses
  - Any other ways to improve the FSC
  - Do you agree / disagree with the suppositions made in the presentation

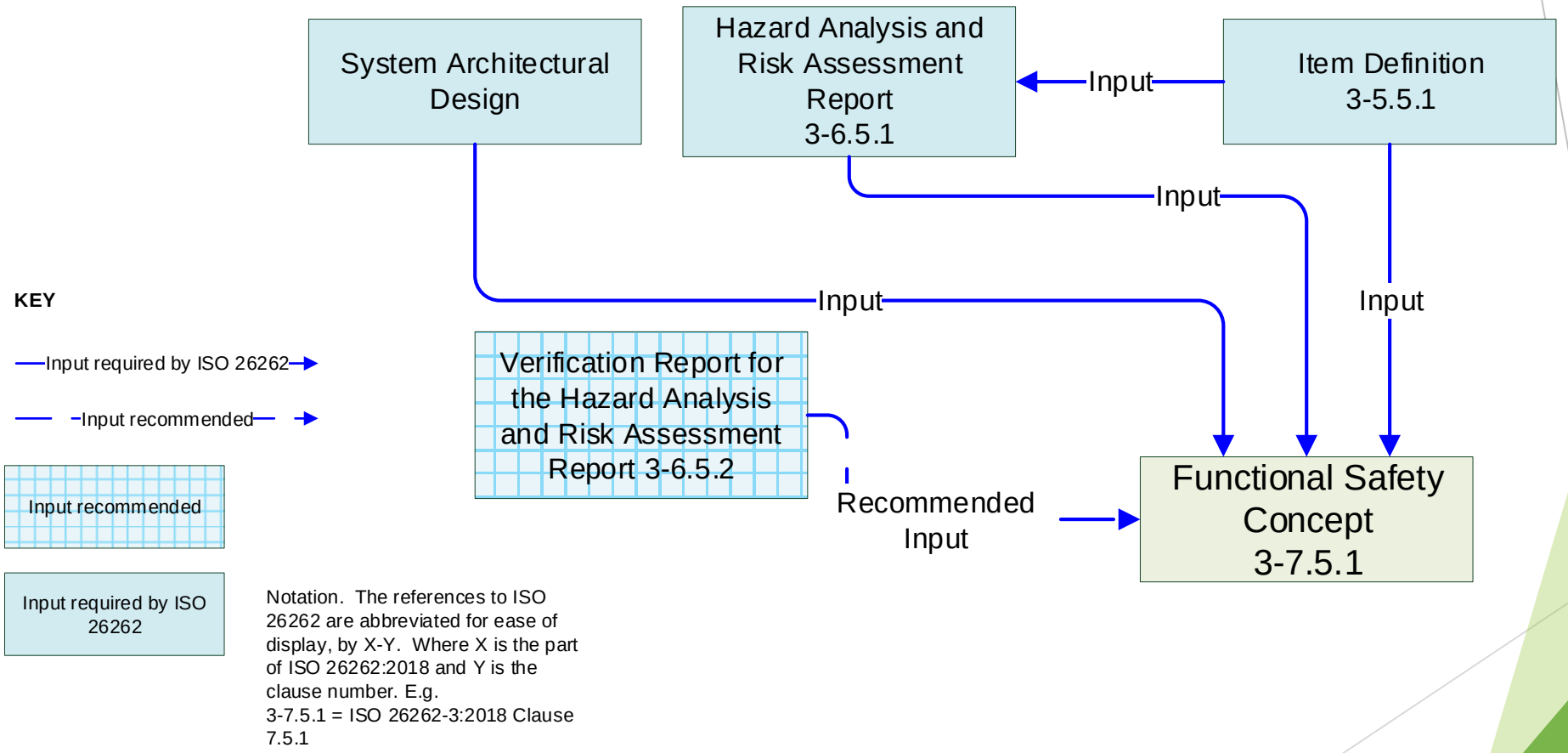
What is required to have a complete and compliant FSC



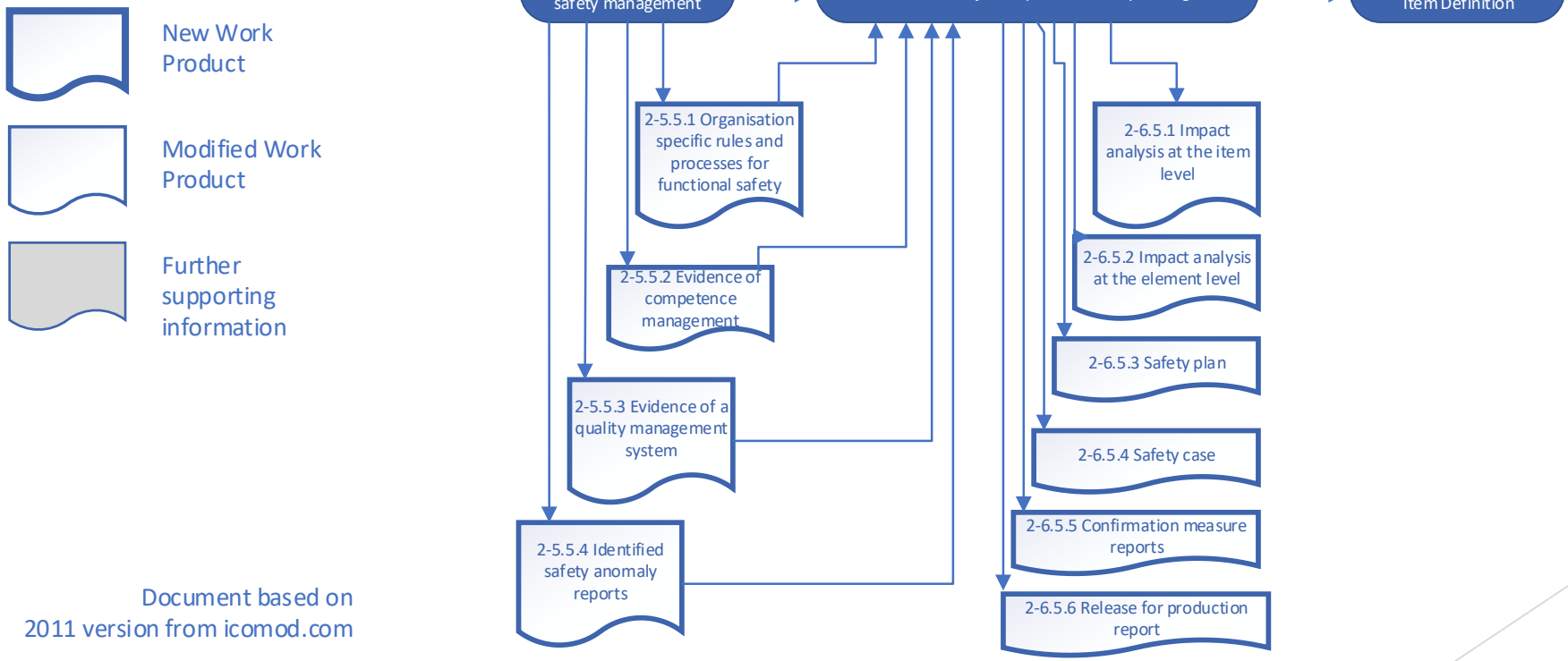
What requirements have to be met by the FSC itself



What are the inputs to the FSC?



What is needed before these inputs?



Document based on 2011 version from icomod.com

Work products from Supporting Processes are also needed

Configuration management plan 8-7.5.1

Supplier Selection Report 8-5.5.1

Change Management Plan 8-8.5.1

Documentation management plan 8-10.5.1

Software tool criteria evaluation report 8-11.5.1

Software tool qualification report 8-11.5.2

Weaknesses observed in FSC development

Part of what is required is either:

- Not completed at all
- Not completed in accordance with the applicable clauses of ISO 26262:2018

AND

ISO 26262:2018 Tailoring Rules are not adhered to:

- Either the tailoring is not detailed at all OR
- Missing an adequate rationale

Examples seen:

- Lack of evidence of competence, for the people working on the FSC
- Verification Report not completed
- No process for completing an FSC / and inconsistency in approach across the organisation
- Validation criteria not specified
- Inadequate inputs
- Downstream activities commence when the FSC is not complete
- Lack of rigour in the development of the FSC.

https://www.linkedin.com/in/mark-cousen-4b13242/

Weakness observed affecting the FSC development

- Development of the FSC stumbles due to presence of unreasonable risks with intended behaviour.
  - Item Definition and System Architectural Design – have not adequately addressed the risks associated with the intended behaviour.

Underlying False Assumption made by Organisations

Constraint common to all vehicle product developments – Time and Resource.

What is best allocation of resource to satisfy all business needs and develop product in shortest possible time.

Applying Theory of Constraints – Eli Goldratt. The false assumption is proposed.

False Assumption - **Testing will find any deficiencies in the requirements and ensure safety.**

- Leads to ‘rushing’ the FSC and making erroneous decisions about inputs, supporting processes, etc that are needed for the FSC.

Why all omissions in the FSC cannot be covered through testing

- "Virtually all accidents involving software stem from unsafe requirements… The most effective approach to dealing with safety of computer controlled systems is to focus on creating the safety related requirements" Nancy Leveson, 2020[1]
- Software related accidents have occurred even when the requirements have been met. Because:
  - The requirements specify behaviour that is not safe from a system perspective
  - The requirements do not specify some behaviour that is required for system safety
  - The s/w has unintended (unsafe) behaviour beyond what is specified in the requirements[2]
- S/W Testing and operational reliability measurement determines if the S/W matches the required behaviour. Not whether that behaviour is safe, if something is missing or whether additional, unspecified behaviour is possible[2]

[1]Inside Risks, Are you sure your software will not kill anyone, Communications of the ACM, Feb 2020, Vol 62, No 2

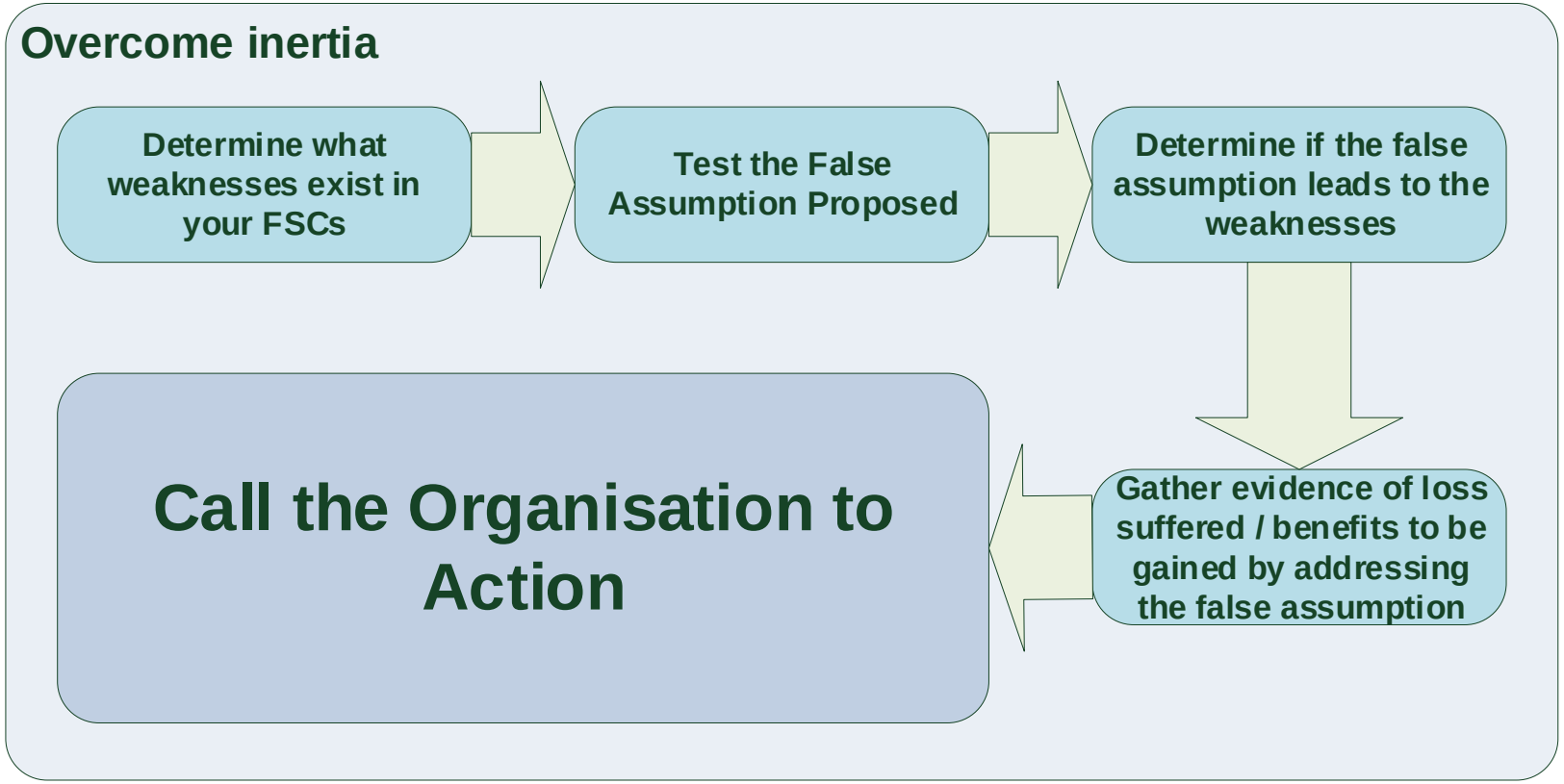
[2]Safeware, System Safety and Computers. Nancy G Leveson

Why is the FSC important

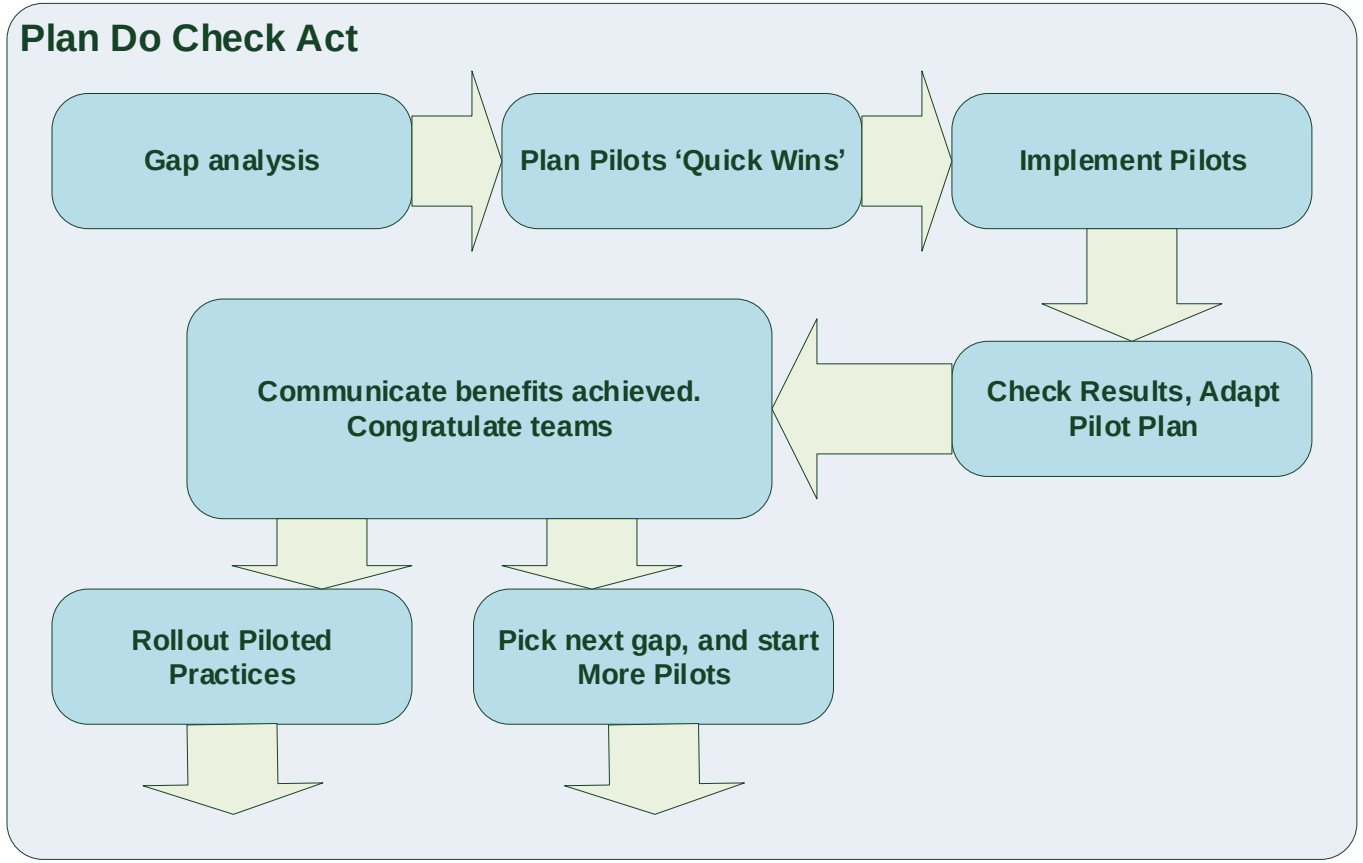
- After the safety goals, the FSC is the most important set of safety requirements to achieve safety when there is a malfunction of a road vehicle e/e system (item).
- No downstream activity can fully cover for deficiencies in the FSC.
- A robust FSC prevents downstream issues, reduces ‘churn’ and has many non-safety related benefits.

https://www.linkedin.com/in/mark-cousen-4b13242/

Solution – Road Map – Call To Action



Solution Road Map
– Plan Do Check Act Deming Circle



https://www.linkedin.com/in/mark-cousen-4b13242/

Recap and Discussion

- Presentation of observations and recommendations
  - What is required for an FSC
  - What are the weaknesses seen in application of ISO 26262 in the development of the FSC
  - What is the false assumption that is suggested to be the root cause of these weaknesses
  - Argumentation why this assumption is false and why it is the root cause
  - Proposed solution
- Discussion of the comments provided by participants.
  - Are there any weaknesses not covered by the false assumptions that are proposed,
  - Are there any other false assumptions made that cause FSC weaknesses
  - Any other ways to improve the FSC
  - Do you agree / disagree with the suppositions made in the presentation

Mark Cousen

Independent Functional Safety Specialist

https://www.linkedin.com/in/mark-cousen-4b13242/