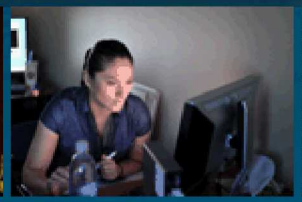
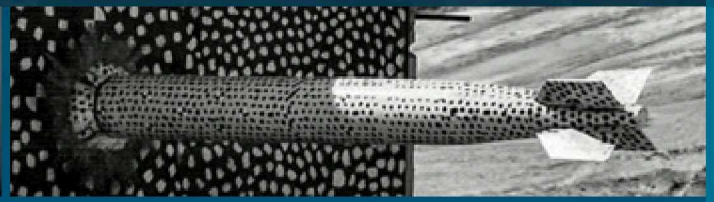
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-5076C

Trusting Embedded Hardware and Software in Treaty Verification Systems





PRESENTED BY

Jay Brotz, Sandia National Laboratories

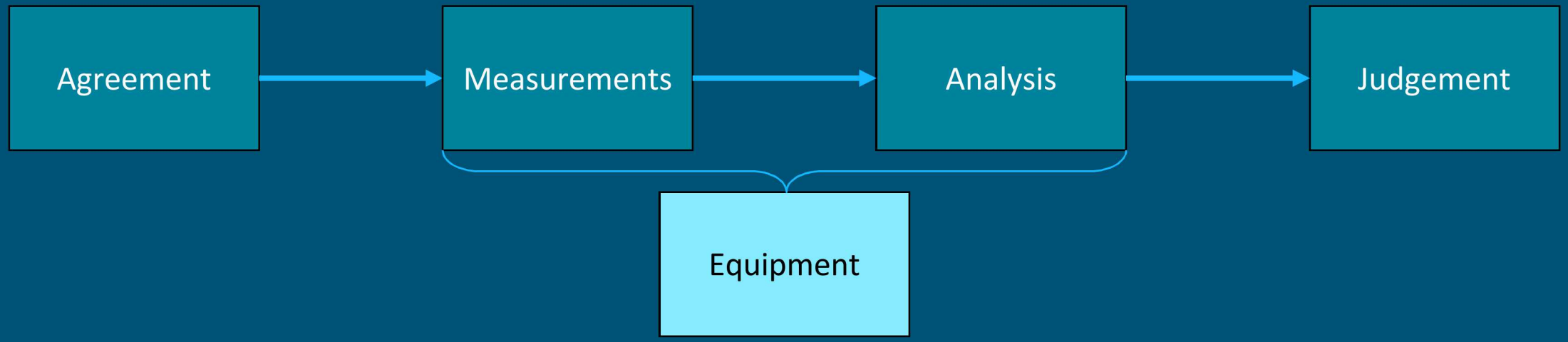
41st ESARDA Annual Meeting

16 May, 2019

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Trusting Hardware and Software in Disarmament Verification Equipment

Treaty verification includes:



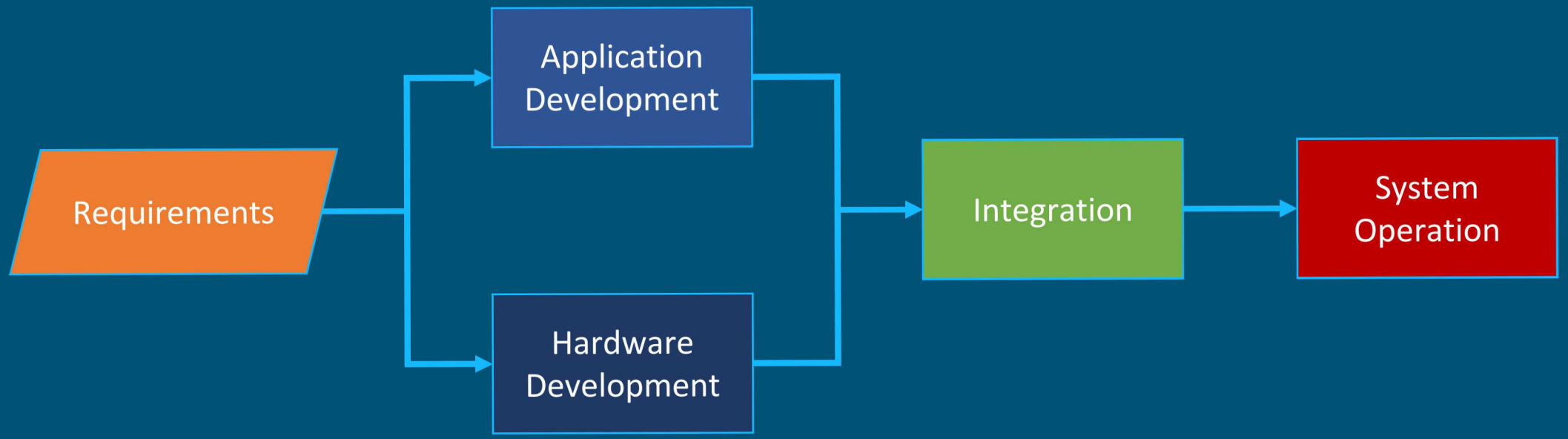
Certification: the process by which the **host** gains confidence in equipment

- Safety
- Security
- Information security

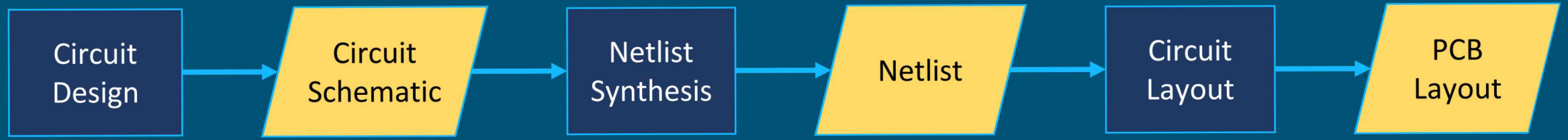
Authentication: the process by which the **monitor** gains confidence in equipment

- Data is correct
- Data is complete

System Development Cycle

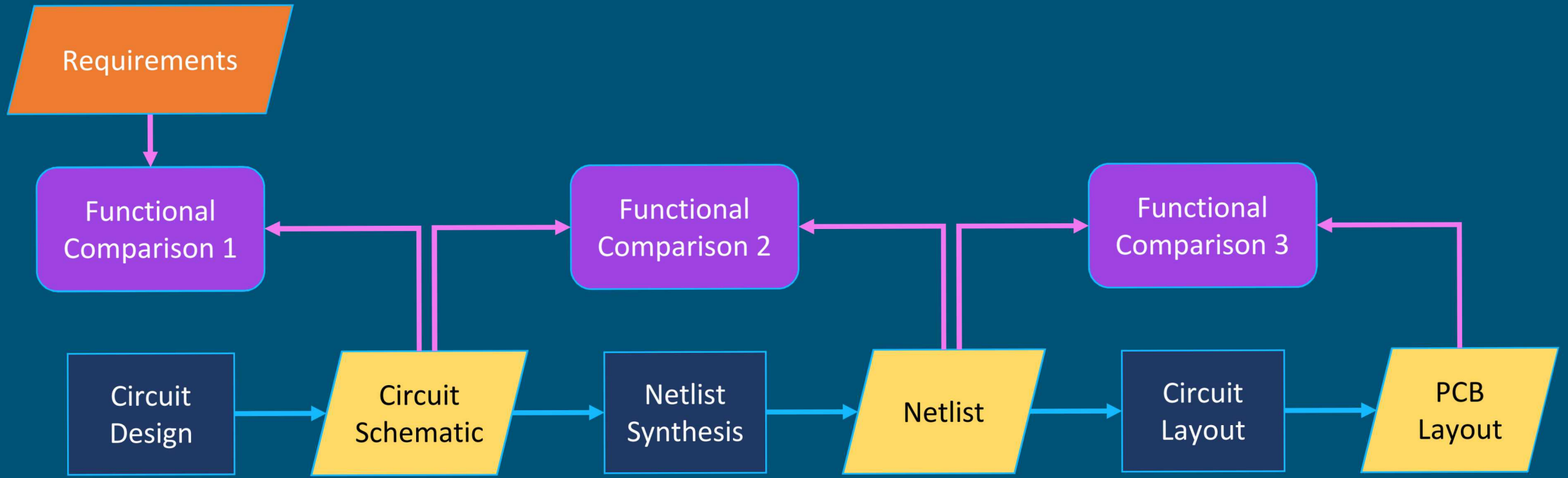


Functional Comparisons



PCB = Printed Circuit Board

Functional Comparisons

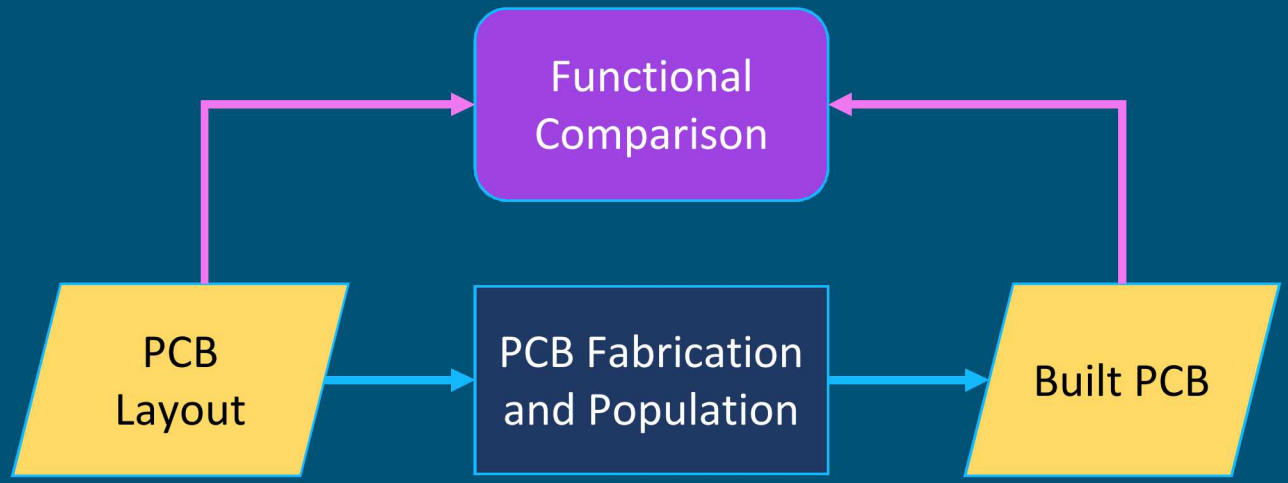


PCB = Printed Circuit Board

Exact Comparisons

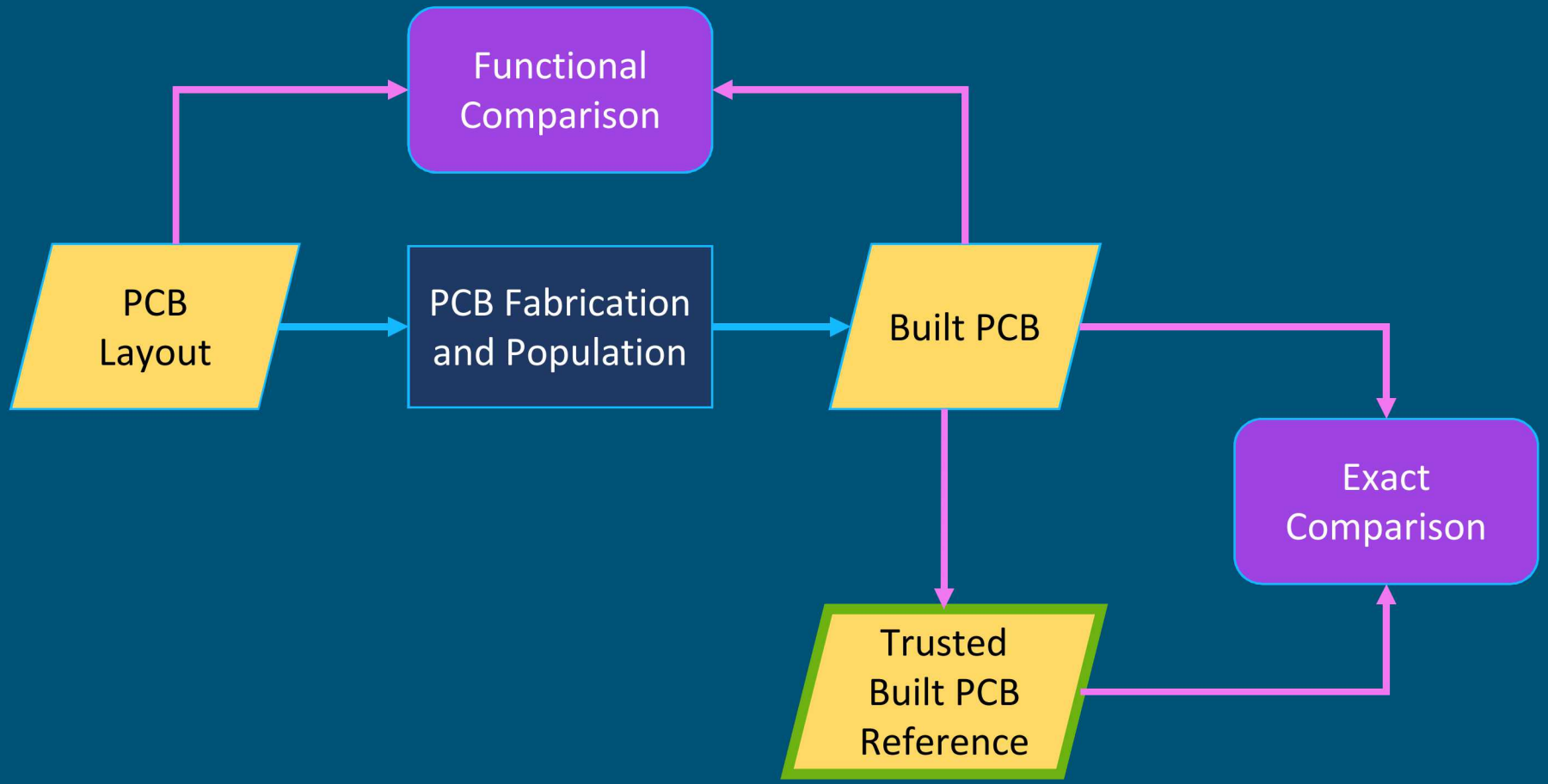
PCB = Printed Circuit Board

Exact Comparisons



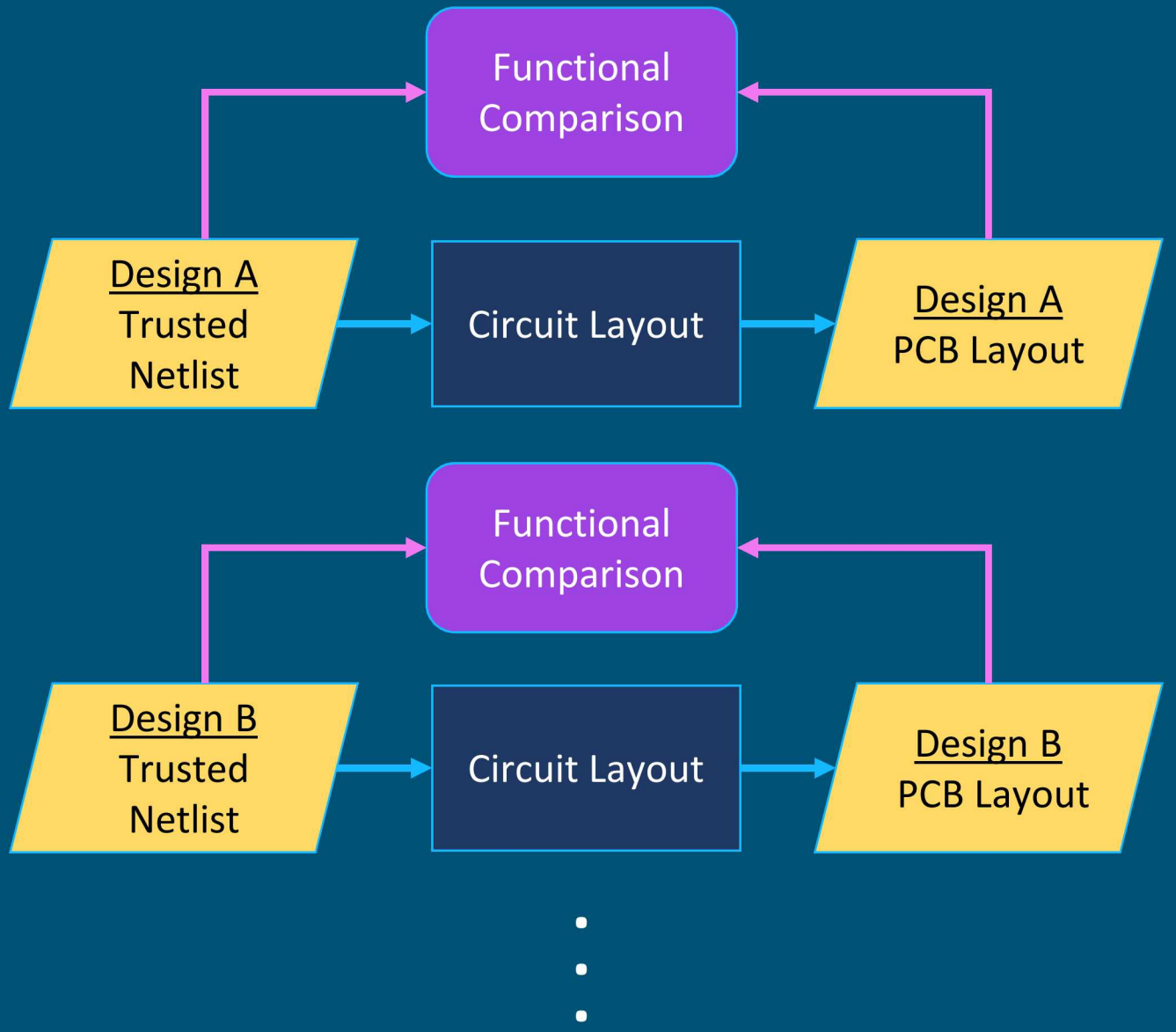
PCB = Printed Circuit Board

Exact Comparisons

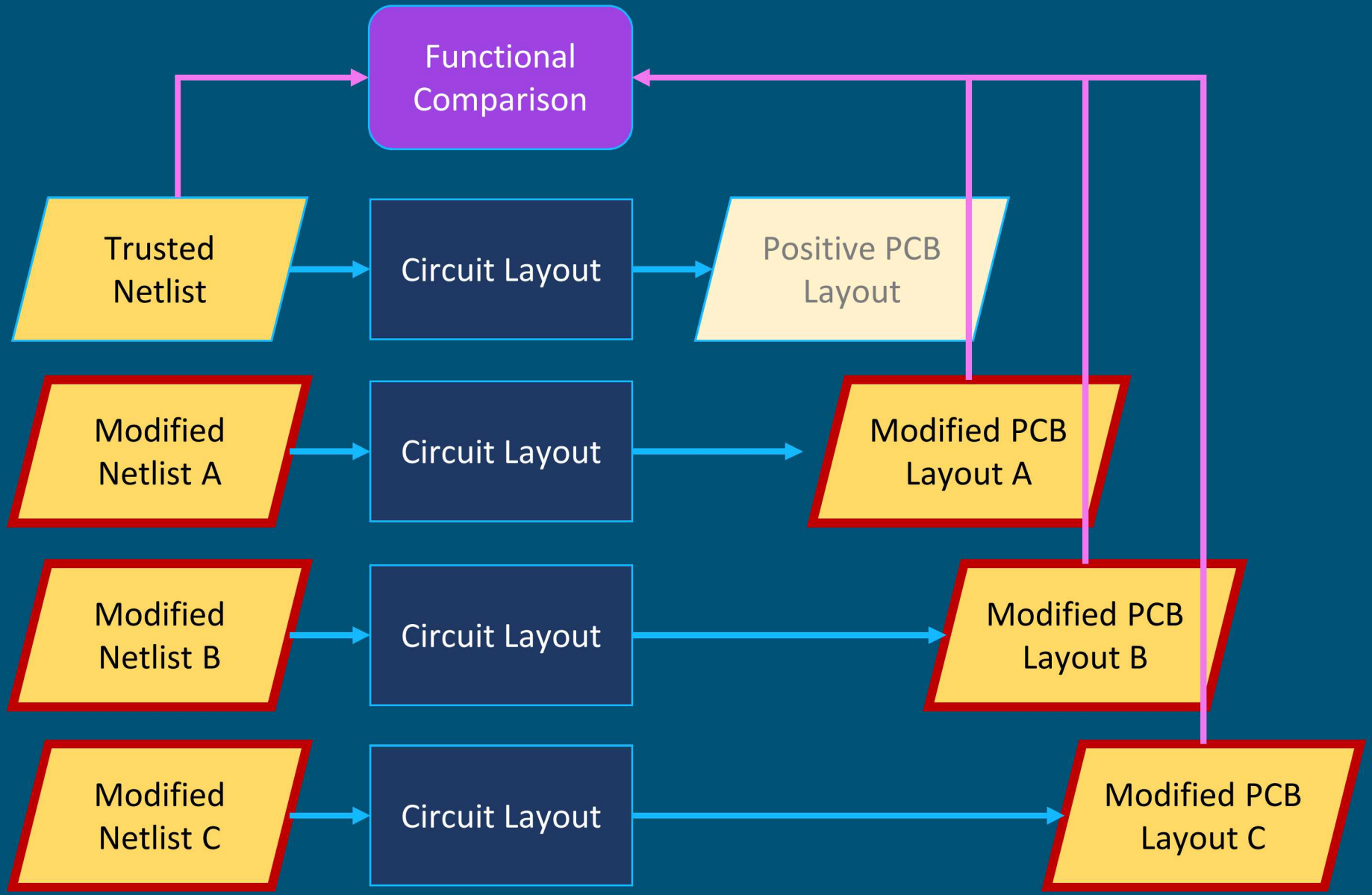


PCB = Printed Circuit Board

Evaluating Functional Comparisons



Evaluating Functional Comparisons



Recommendations

Functional comparison methods should be adapted from other industries, such as hardware error control in the integrated circuit industry.

Authentication and certification methods should be researched and developed alongside treaty verification equipment.

These two areas of R&D could be pursued as inter-organization, or international, collaborations.