Certification and Assurance Cases

Paul L. Jones
OSEL/CDRH/FDA

Terminology

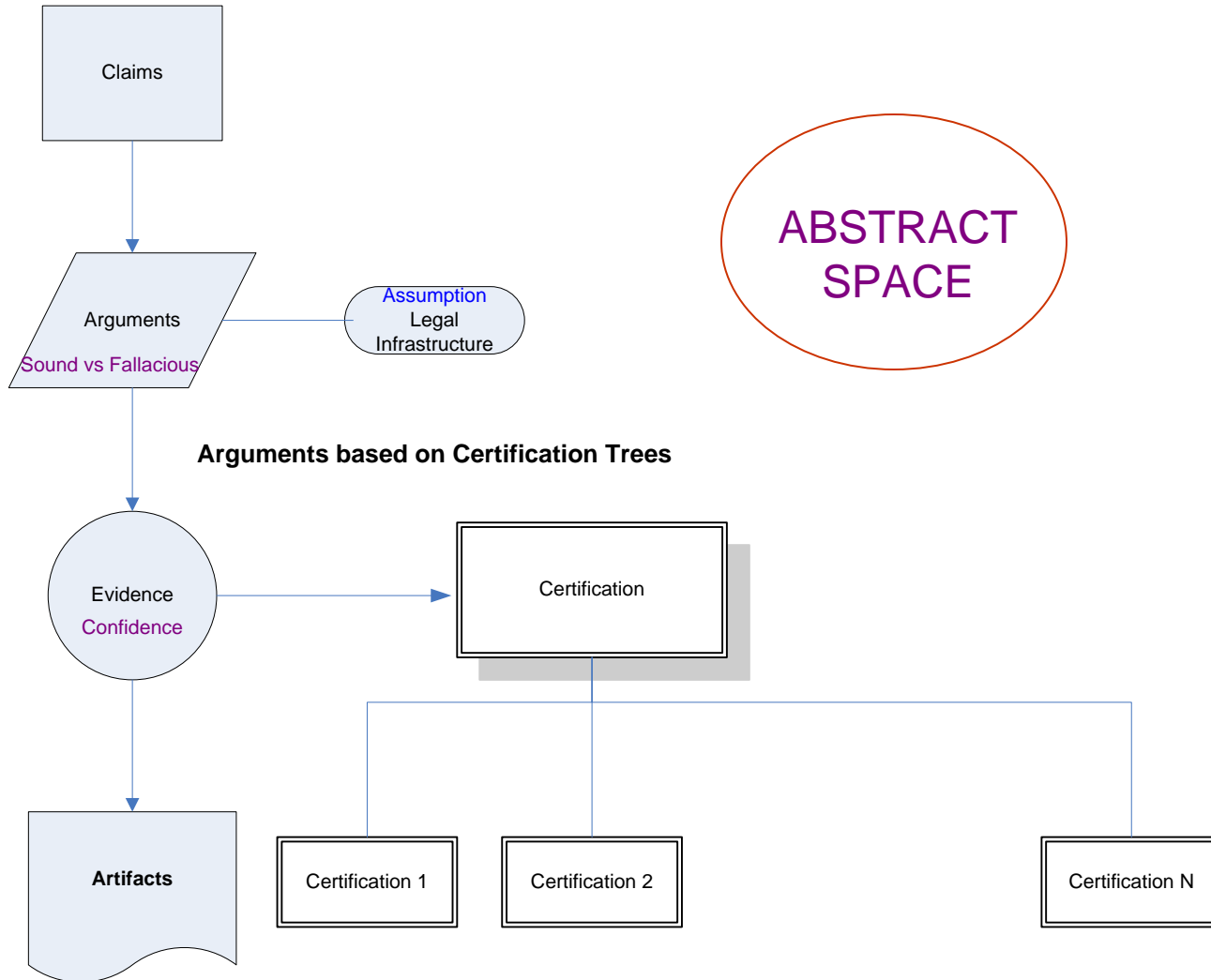*Certification*:

Officially recognize (someone or something) as possessing certain qualifications or meeting certain "standards".
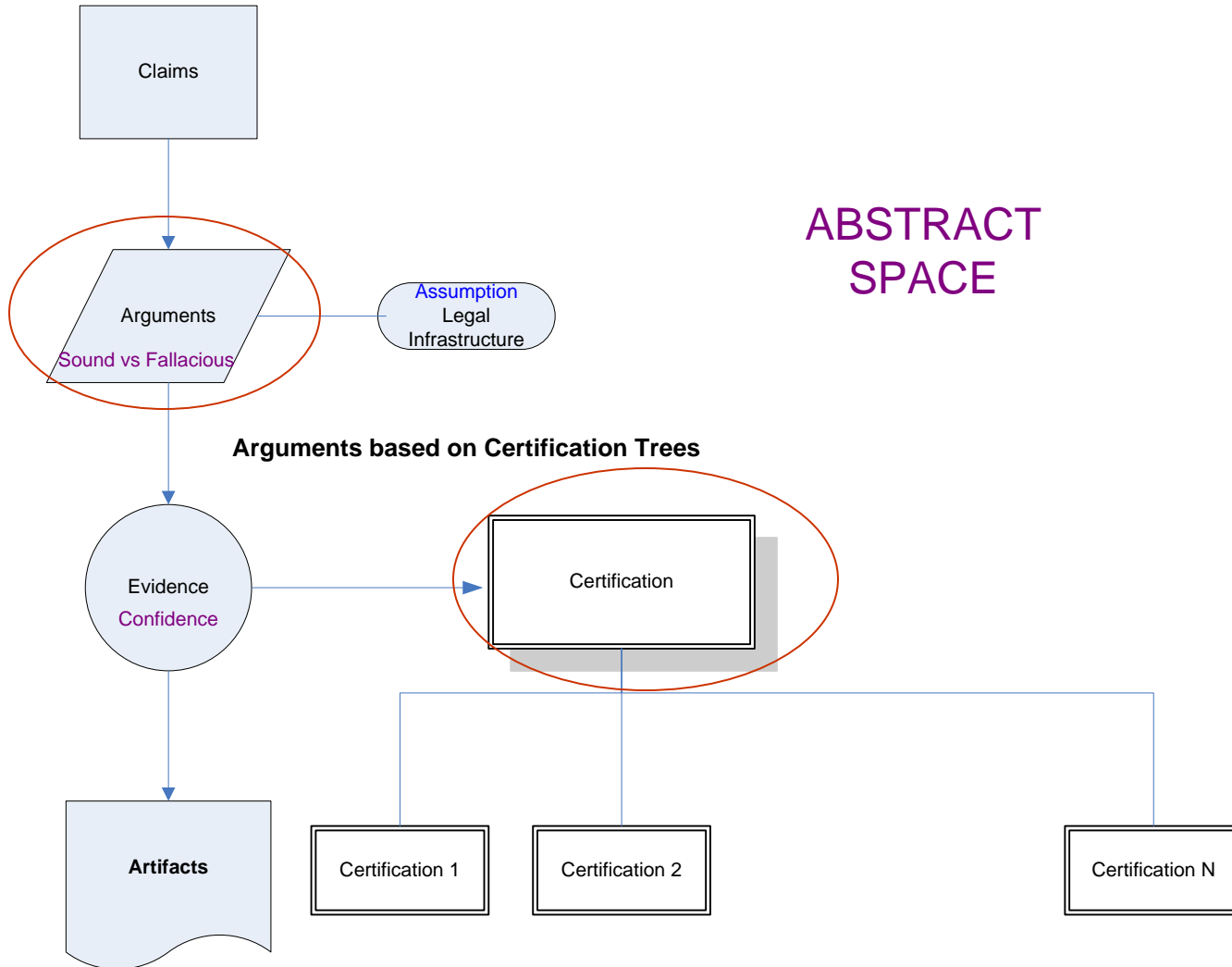
Evidence:

In its broadest sense includes everything that is used to determine or demonstrate the truth of an assertion (claim).

Assurance Case Framework

Claims

Arguments

Sound vs Fallacious

Assumption
Legal
Infrastructure

ABSTRACT
SPACE

Arguments based on Certification Trees

Evidence
Confidence

Certification

Artifacts

Certification 1

Certification 2

Certification N

Assurance Case Framework

Claims

Arguments

Sound vs Fallacious

Assumption
Legal
Infrastructure

ABSTRACT
SPACE

Arguments based on Certification Trees

Evidence
Confidence

Certification

Artifacts

Certification 1
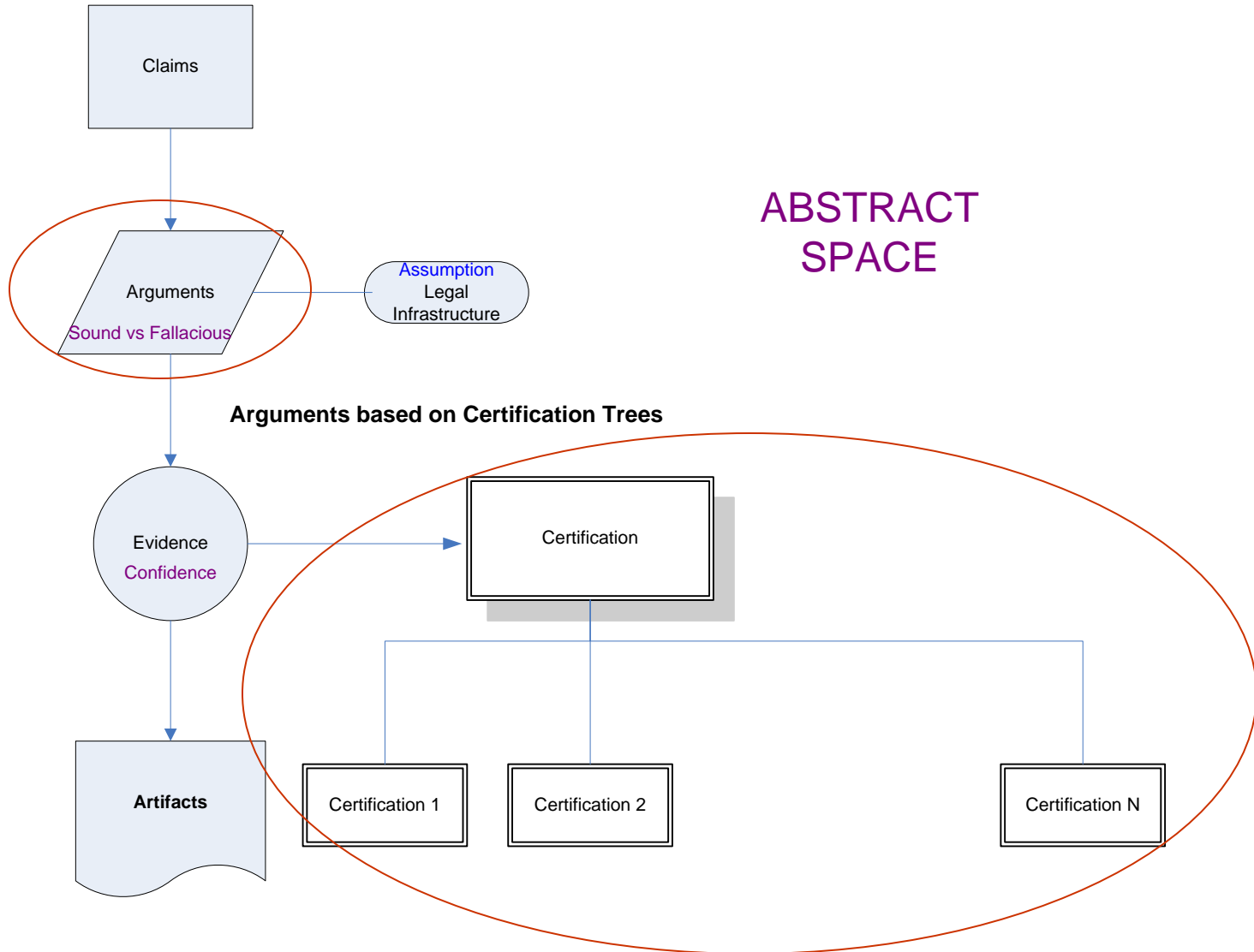
Certification 2

Certification N

Certification based arguments

Specious / Fallacious argument based on a Certification

We have been certified as conforming to ISO 9001 therefore we produce quality products + a certification letter.

Assurance Case Framework

Claims

Arguments

Sound vs Fallacious

Assumption
Legal
Infrastructure

ABSTRACT
SPACE

Arguments based on Certification Trees

Evidence
Confidence

Certification

Artifacts

Certification 1

Certification 2

Certification N

Certification based arguments

Specious / Fallacious arguments based on certifications

We conform to the IEC 62304 medical device SDLC process standard therefore our medical device software is safe

[in addition]

We conform to the ISO 14971 medical device risk management (process) standard therefore our device is "very" safe!
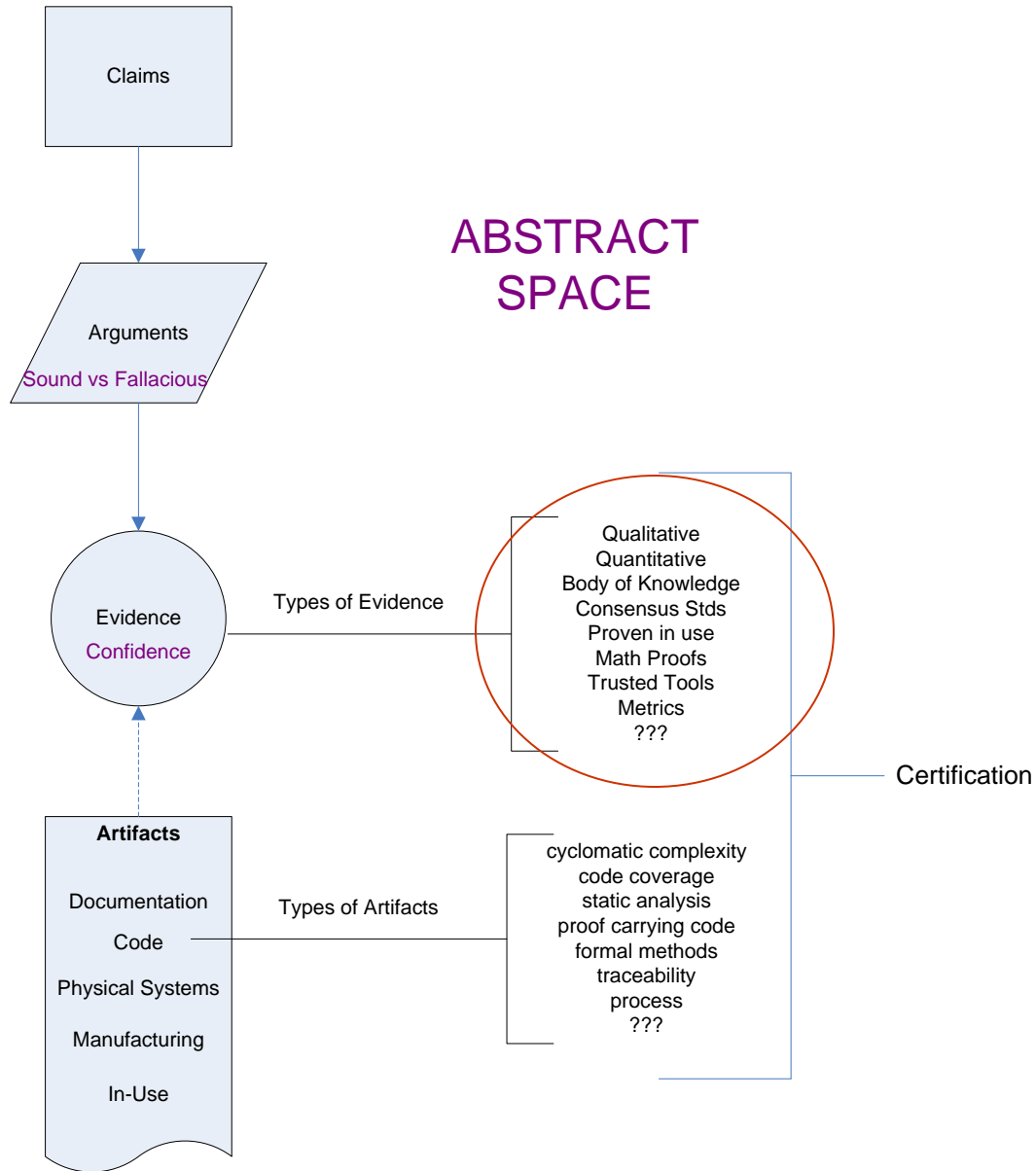
Certification based arguments

Trustable argument based on certification

Our attachment plugs and receptacles are electrically safe because they conform to the UL 498 standard + letter of certification from Underwriters Laboratories.

What can be certified about software?

Assurance Case Framework

Claims

Arguments
Sound vs Fallacious

ABSTRACT
SPACE

Evidence
Confidence

Types of Evidence

Qualitative
Quantitative
Body of Knowledge
Consensus Stds
Proven in use
Math Proofs
Trusted Tools
Metrics
???

Certification

Artifacts

Documentation

Code

Physical Systems

Manufacturing

In-Use

Types of Artifacts

cyclomatic complexity
code coverage
static analysis
proof carrying code
formal methods
traceability
process
???

Assurance Case Framework

Claims

Arguments
Sound vs Fallacious

ABSTRACT
SPACE

Evidence
Confidence

Types of Evidence

Qualitative
Quantitative
Body of Knowledge
Consensus Stds
Proven in use
Math Proofs
Trusted Tools
Metrics
???

Certification

Artifacts

Documentation

Code

Physical Systems

Manufacturing

In-Use

Types of Artifacts

cyclomatic complexity
code coverage
static analysis
proof carrying code
formal methods
traceability
process
???

Conclusion 1

Regulators need well defined certification protocols and legal infrastructure to enable trust in assurance cases which are necessarily abstract.

Conclusion 2

Need to evolve software engineering to include trusted tool chains, principled practices, and meaningful metrics that establish trustable evidence as a product is developed and maintained.