IEEE SA
STANDARDS ASSOCIATION

IEEE WORKING GROUP FOR RESILIENT USER EQUIPMENT IN POSITIONING, NAVIGATION, AND TIMING (P1952)

IEEE STANDARDS DEVELOPMENT

8 May 2024

Douglas Arnold, Meinberg USA

Shelby Savage, Patricia Larkoski, Homeland Security Systems Engineering & Development Institute, an FFRDC operated by The MITRE Corporation for the Department of Homeland Security

Stephen Guendert, IBM Corporation

Marc Weiss, Marc Weiss Consulting

Cristina Seibert, NextNav LLC

David Sohn, Safran

Approved for Public Release
Distribution Unlimited
Public Release Case Number 24-1035

IEEE

CONTEXT FOR RESILIENT PNT (POSITION, NAVIGATION, AND TIMING)

- **No generally accepted standard of "resilient PNT user equipment (UE)"**

- **Resilience is "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, et al.)**
  - "Assurance" is the ability to establish confidence in UE performance
  - "Reliability" is the ability to function properly (not correctly) under specified conditions
  - "Robustness" is the ability to function correctly under specified conditions, including under adversity
  - "Resilience" is the ability to function correctly under *unanticipated adverse conditions through adjustment and adaptation*

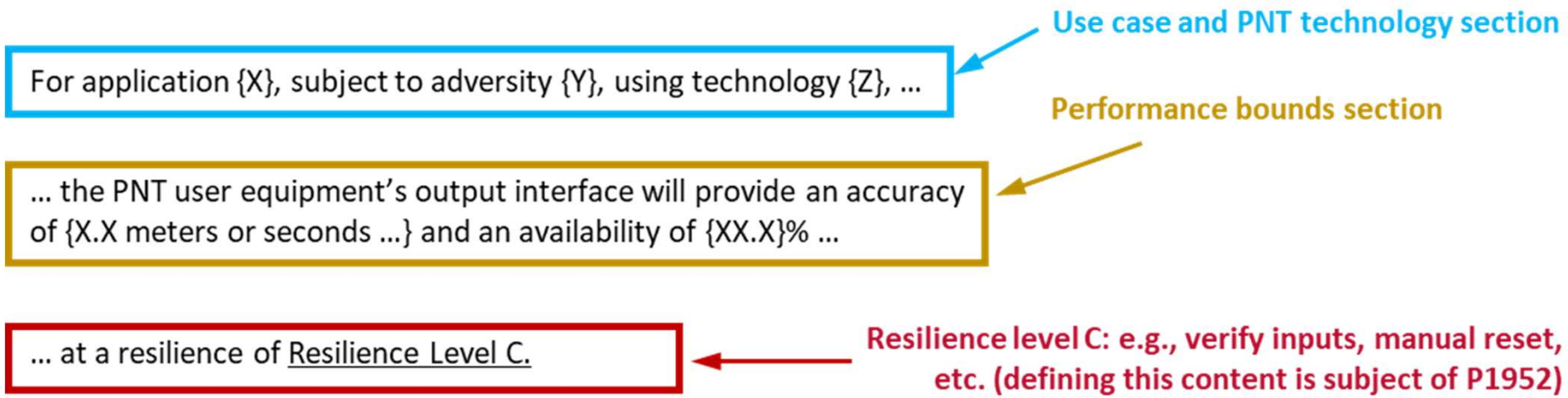
- **Resilience contains several concepts: "ability of a system to anticipate and withstand external shocks, bounce back to its pre-shock state as quickly as possible and adapt to be better prepared to future catastrophic events" (Mathaios Panteli, et al, 2017)**

KEY PRINCIPLES OF P1952 (OUR GUIDES TO ACHIEVE P1952'S GOALS)

- **Many concepts come from the "Resilient PNT Conformance Framework," developed by many PNT stakeholders led by US Department of Homeland Security (DHS)**
- **Key Concepts**
  - Outcome-based: focus is on boundary of PNT UE, not internals (allowing innovation)
  - Generalized: independent (if possible) to threat type, use case, etc.
  - Cumulative: successive resilience levels build upon previous ones
- **Desired outcomes**
  - Voluntary standard defining a common language of resilience
  - Focus on requiring resilient behaviors organized in levels of increasing resilience, allowing user to choose level appropriate for their application
- **Some limits to P1952's work**
  - P1952 is limited to UE; no requirements on infrastructure, like GPS satellites, radio beacons, etc.
  - Comm links between PNT UE boxes are left to comm-specific standards
  - P1952 won't set things like accuracy requirements (the user must fill those in)

RESILIENCE LEVELS AND STAKEHOLDER COMMUNICATION

- P1952 will define Resilience in terms of a UE box's behavior under disruption
- Resilience is not described in terms of the usual performance metrics (1-m of accuracy, 1 ms/month of drift, etc.), so P1952 will not make such requirements
- Standard will allow statements like this:



P1952 OUTLINE

1. **Overview and Scope**
   Scope of P1952, brief discussion of the general definition of resilience
2. **Normative References**
   List of required refs for P1952 execution
3. **Definitions, Acronyms, & Abbreviations**
   Brief definitions of key terminology that will be given more detailed descriptions in later clauses
4. **Conventions**
   Language & symbol conventions, including for normative words (“should”, “shall”, …)
5. **Key Concepts**
   Principles guiding P1952 (e.g., P1952’s focus on the boundary of the UE and on UE behavior)
6. **PNT User Equipment Model**
   General model of PNT UE

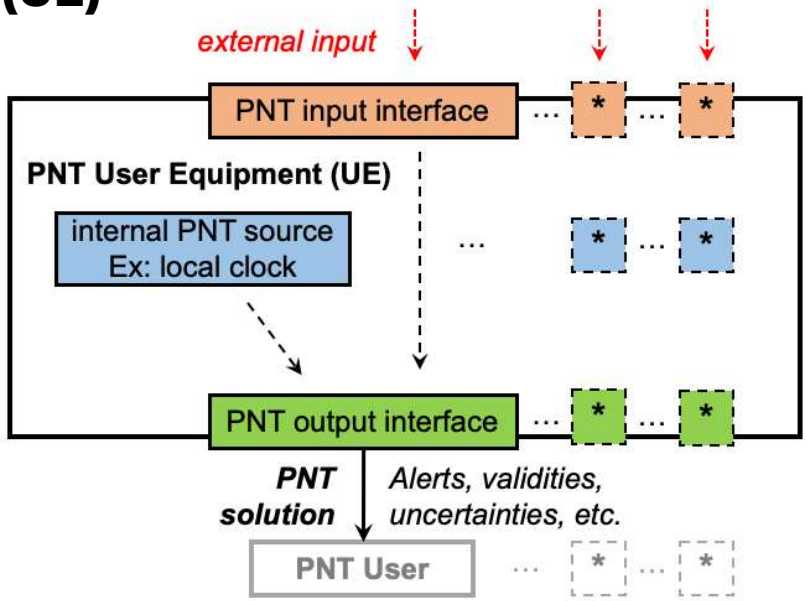
These clauses contain the technical concepts that are most relevant to the detailed definition of resilience

7. **Threat & Disruption Models**
   General model or categorization of threats
8. **Resilience Levels**
   Definition of requirements organized into resilience levels
9. **Product Implementation Conformance Statements**

A. **Annex – Example Architectures**
   Examples of resilient UE architectures
B. **Annex – Use Case Scenarios, Threats, and Examples**
   General use-case concepts & description of important and representative use cases
C. **Annex – Best Practices for Resilient PNT UE**
D. **Annex – Evaluation Guidelines**
E. **Annex – Bibliography**

CLAUSE 6 – MODEL FOR PNT USER EQUIPMENT (UE)

- **P1952 is focused on the input and output interfaces of the UE**
  - Placing requirements on interfaces rather than UE internals will foster innovation
  - Some thought has been given to networked UE as well, but how far we will take this remains to be seen
- **P1952 is only concerned with PNT interfaces, not any interface**
  - P1952 is not concerned, for example, with power surges at power interfaces
  - Probably, P1952 will limit itself to functioning interfaces, so resilience to physical damage will be out of scope



* The generic PNT UE Model can encompass any number of input interfaces, internal PNT sources, output interfaces, and PNT users.

- **Clause 6 does include possibility of network interfaces between PNT UE boxes**
  - Example is Precision Time Protocol (PTP)
  - Requirements for such wide-area systems have proven challenging
  - Clause 6 distinguishes between 1) wide-area networking of PNT UE boxes and 2) local “integration” of PNT UE boxes on a single “installation”

CLAUSE 7 – THREAT CATEGORIZATION

- **Purpose: Rationalize threat space so users & testers don't need to consider threats one-by-one**
  - Organize the threats against PNT UE into categories
  - Proposed organizing principles include effect of threat on UE (output interface), attack vector of threat (input interface), and by test methods

- **Requirements in Clause 8 will reference threat categories in Clause 7**
  - Current Clause 7 draft organizes threats in a matrix of 2 dimensions:
    - 1st dimension: which PNT interface is being attacked (radio interface, optical, time network, …)
    - 2nd dimension: how is the PNT interface being attacked (noise interference, added signal delay, …)
  - Each item in 2nd dim. also has a typical effect on UE, so clause is also partly outcome-based
  - Some difficulties: 1) Some spoofers also use jammers (so two categories at once); arguably, this is primarily spoofing; 2) different users might have very different needs, so there is a danger of forcing one-size-fits-all

CATEGORIZATION OF THREATS

2) How is the PNT interface disturbed?

1) What is the PNT interface technology?

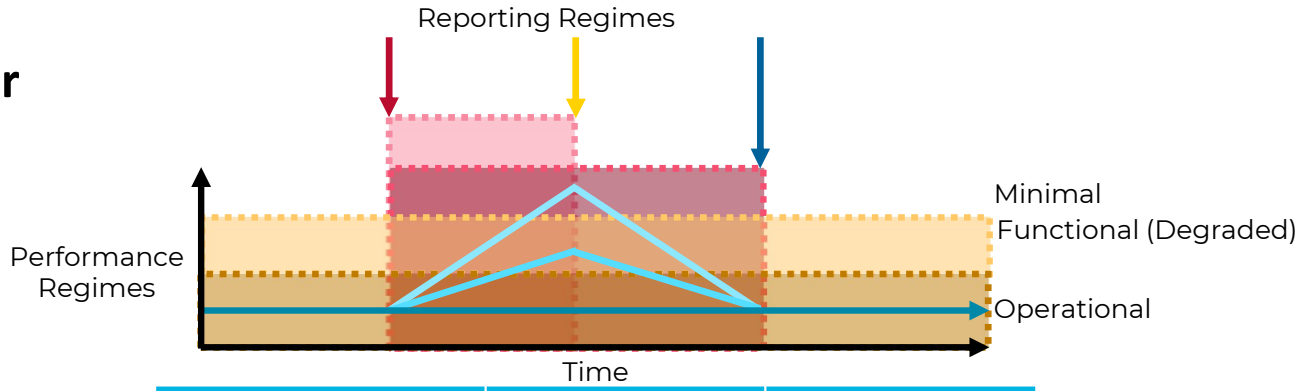
PNT UE Interface Categories	Threat, Hazard, and Disruption (THD) Main Categories					
	Interference	PNT Signal Attenuation	PNT Signal Delay	PNT Data	UE Power	UE Operating State
PNT RF Broadcast	A_1	B_1	C_1	D_1	E_1	F_1
PNT Comms	A_2	B_2	C_2	D_2	E_2	F_2
PNT PSP	A_3	B_3	C_3	D_3	E_3	F_3
PNT Vision	A_4	B_4	C_4	D_4	E_4	F_4
PNT Magnetic	A_5	B_5	C_5	D_5	E_5	F_5
PNT Inertial	A_6	B_6	C_6	D_6	E_6	F_6
PNT Air Pressure	A_7	B_7	C_7	D_7	E_7	F_7
PNT UE Ambient	A_8	B_8	C_8	D_8	E_8	F_8
PNT UE Management	A_9	B_9	C_9	D_9	E_9	F_9

CLAUSE 8 – RESILIENCE LEVELS

Proposed Resilience Levels per current draft:

1. Detect and Alert (alert and reset requirements)
2. Recover (recover to operational resilience category)
3. Resist (maintain functional resilience category through “holdover”)
4. Withstand (maintain operational resilience category through adversity)
5. Verify (outlier detection)

Allows for declaration of capability list(s) including adversities against which resilience level(s) can be supported by PNT UE



Minimal requirements**	Functional requirements	Operational requirements
Accuracy, Precision	Accuracy, Precision (threshold)	Accuracy, Precision (objective)
Availability	Availability (threshold)	Availability (objective)
Integrity	Integrity (AL, IR, TTA)	Integrity (AL, IR, TTA)
Continuity	Continuity (threshold)	Continuity (objective)
Coverage	Coverage (threshold)	Coverage (objective)
Recovery Time	Recovery Time	Recovery Time
	Holdover Time	Holdover Time
Reset Operation	Reset Operation	Reset Operation
Report Interface Incompatibility	Report Interface Incompatibility	Report Interface Incompatibility
Report Integrity Events	Report Integrity Events	Report Integrity Events

**Some or all perf. req. may not meet threshold or objective targets during or after a THD event
Note: depending on the supported use case, not all requirements may be specified

CLAUSE B – USE CASE SCENARIOS, THREATS, AND EXAMPLES

- **Purpose: Provide worked examples demonstrating the usage and application of the standard**
  - All examples are non-normative
  - Not intended to cover all implementations of use cases described
  - Representative use cases from some critical infrastructure sectors
  - Cover all required elements and mix of optional elements from Clause 8

- **Use Case Structure**
  - Description of use case w/ assumptions and context
  - PNT UE input and output interfaces
  - PNT UE performance requirements
  - Use case diagram
  - Representative adversities affecting PNT UE
  - Application of PNT UE performance in relation to resilience levels covered in Clause 8

IEEE SA COPYRIGHT POLICY

By participating in this activity, you agree to comply with the IEEE Code of Ethics, all applicable laws, and all IEEE policies and procedures including, but not limited to, the IEEE SA Copyright Policy.

- Previously Published material (copyright assertion indicated) shall not be presented/submitted to the Working Group nor incorporated into a Working Group draft unless permission is granted.
- Prior to presentation or submission, you shall notify the Working Group Chair of previously Published material and should assist the Chair in obtaining copyright permission acceptable to IEEE SA.
- For material that is not previously Published, IEEE is automatically granted a license to use any material that is presented or submitted.

ACKNOWLEDGEMENT FOR DHS SPONSORED TASKS

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract 70RSAT20D00000001.

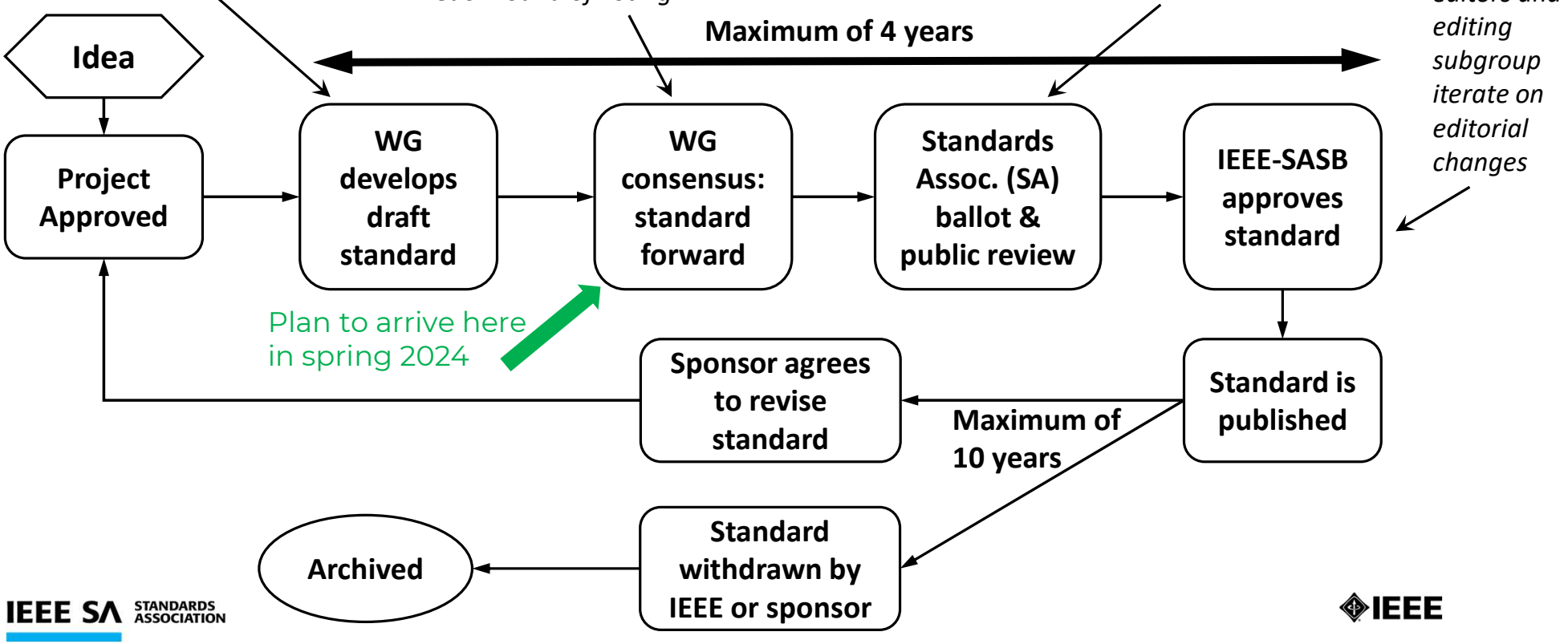
The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task 70RSAT20FR0000062, Next Generation Resilient Position, Navigation, and Timing (PNT).

The results presented in this report do not necessarily reflect official DHS opinion or policy.

BACKUP SLIDES

IEEE STANDARDS PROCESS FOR P1952 WORKING GROUP (WG)

1. *Subgroups create draft clauses*
2. *Editor compiles clauses into draft standard*
3. *P1952 members make comments that are resolved in editing subgroup*
4. *P1952 members vote till two-thirds approve, sending new comments in each round of voting*
5. *Similarly, the SA voting pool has cycles of comments and voting until there is no tech. comment or a 75% vote in favor (editing subgroup resolves comments)*
6. *Finally, SA editors and editing subgroup iterate on editorial changes*



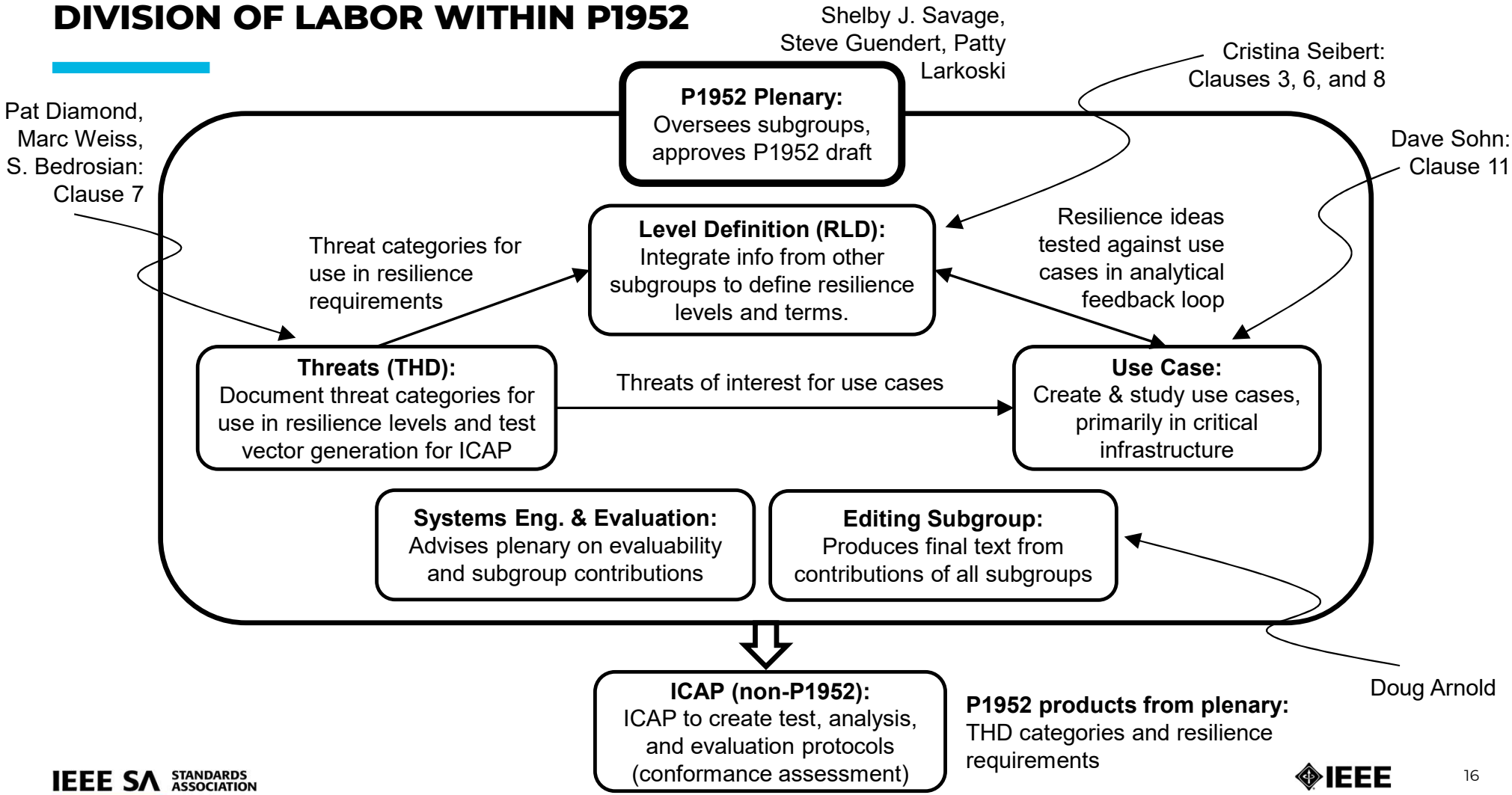
IEEE SA STANDARDS ASSOCIATION

IEEE

CLAUSE 9: PRODUCT IMPLEMENTATION CONFORMANCE STATEMENT (PICS)

Item	Feature	Status	Reference	Comments	Support (Y/N)
RL	Resilience Levels				
RL 1	Resilience Level 1	M	8.2.1		
RL 1.1	Detect THD events and issue alerts when the integrity of the PNT solution could be compromised, at associated false alarm, missed detection and time to alert requirements for the supported PNT	M	8.2.1	PNT UE provider may declare capability list with THD events against which RL 1.1 can be met. When some requirements (e.g. time to alert) are not specified for a supported PNT application or service,	
RL 4.3	Report THD events that the PNT UE can withstand	RL 4:M RL 5:M	8.2.4	PNT UE provider may declare capability list with THD events against which RL 4.3 can be met.	

DIVISION OF LABOR WITHIN P1952



IMPORTANT LINKS AT IMEET

- **Every plenary agenda includes links to important P1952 documents:**
- **iMeet is where members contribute text for consideration & to make comments**
  - If you want to contribute and are confused, please reach out to relevant contact (see P1952 organization chart in slide below)

Links:

- Introduction and Current Status of P1952 **(These slides)**
- P1952 Project Authorization Request **(IEEE document defining P1952's scope)**
- P1952 Policies & Procedures **(P1952's governing document)**
- P1952 Outline **(Proposed outline for P1952 standard)**
- Draft Clauses **(Current drafts of P1952 clauses)**
- Terminology **(Draft of Terminology)**
- P1952 Organization & Protocols **(Organization of subgroups and submission protocols)**
- Clause Assignments **(Points of contact and goal dates for each clause)**
- Resilient PNT Conformance Framework **(DHS-sponsored multi-stakeholder document on Resilient PNT, 2021)**
- Drafting and Editing Process **(Description of the IEEE drafting and editing process)**