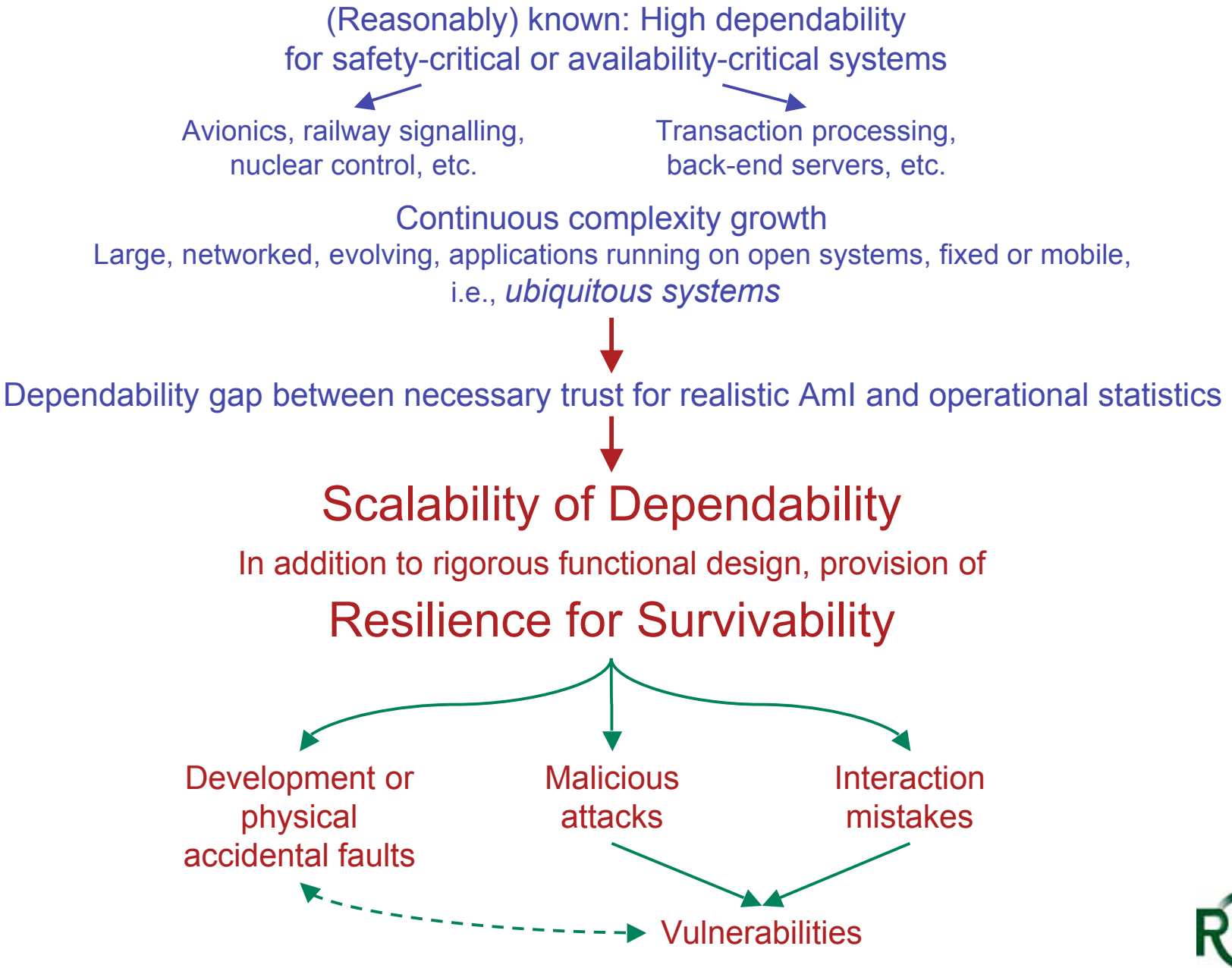
ReSIST

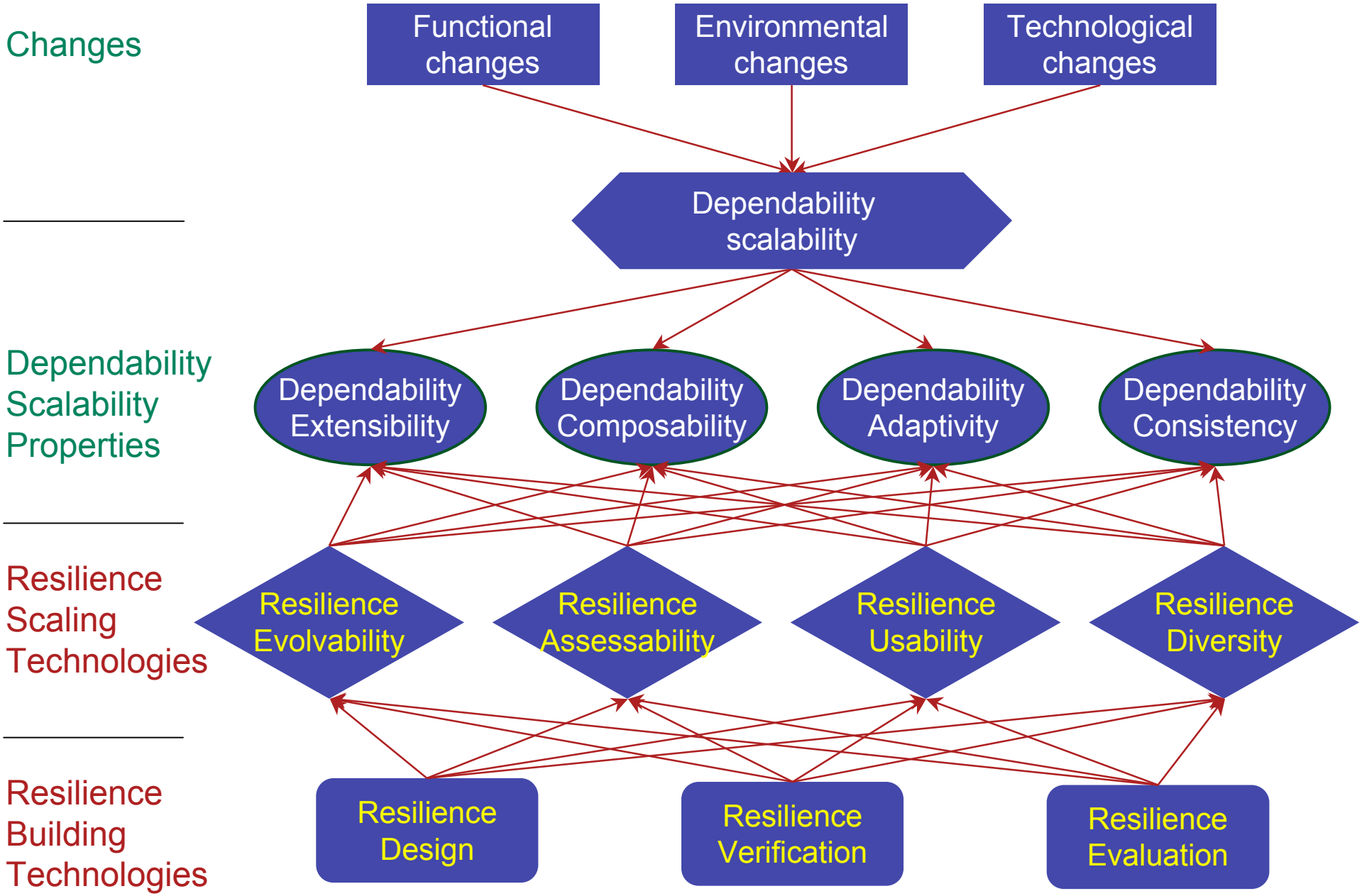
Resilience for Survivability in IST

A European Network of Excellence

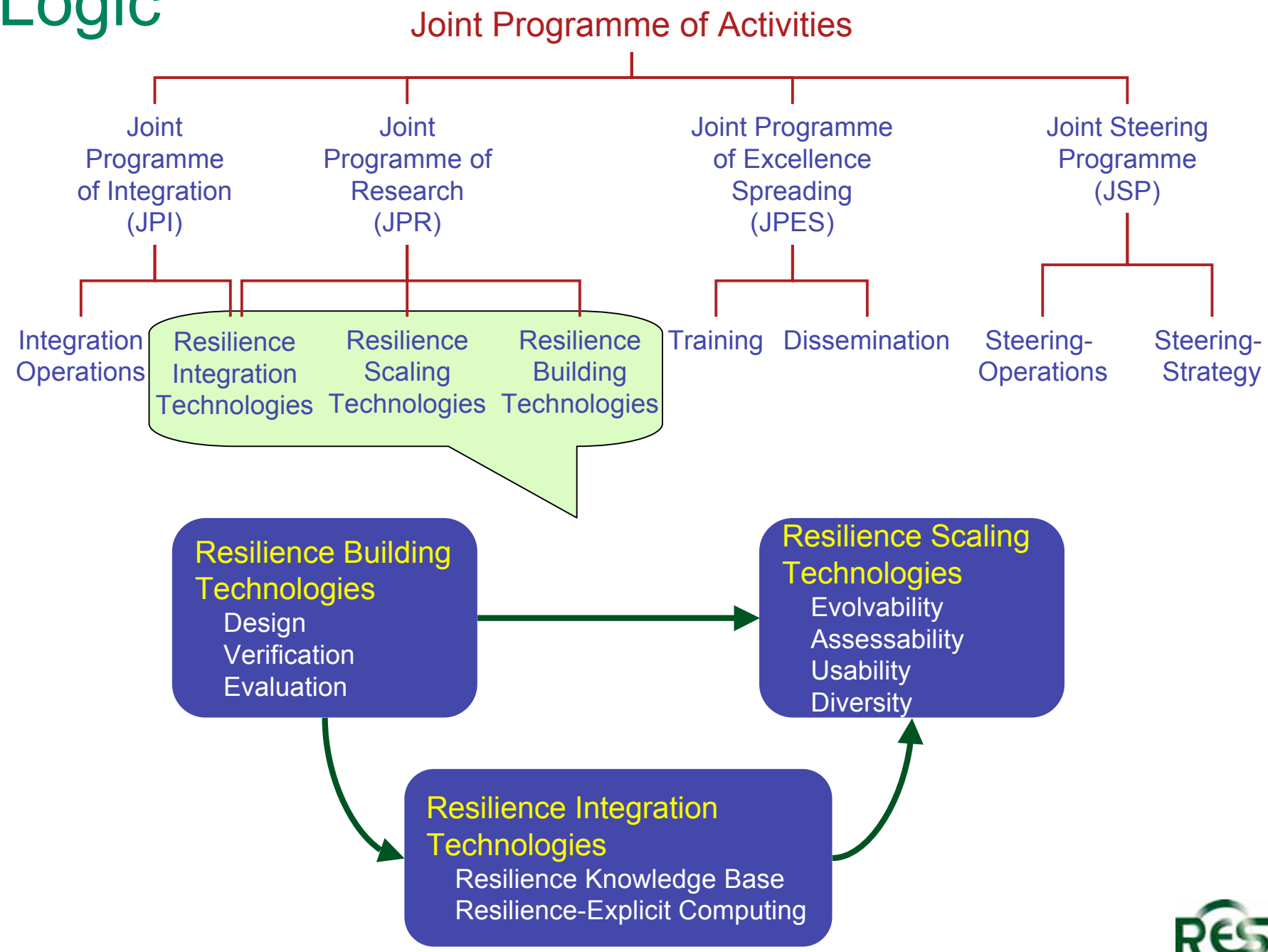
- Rationale
- Logic
- Joint Programme of Activities insight
- Partnership

Rationale

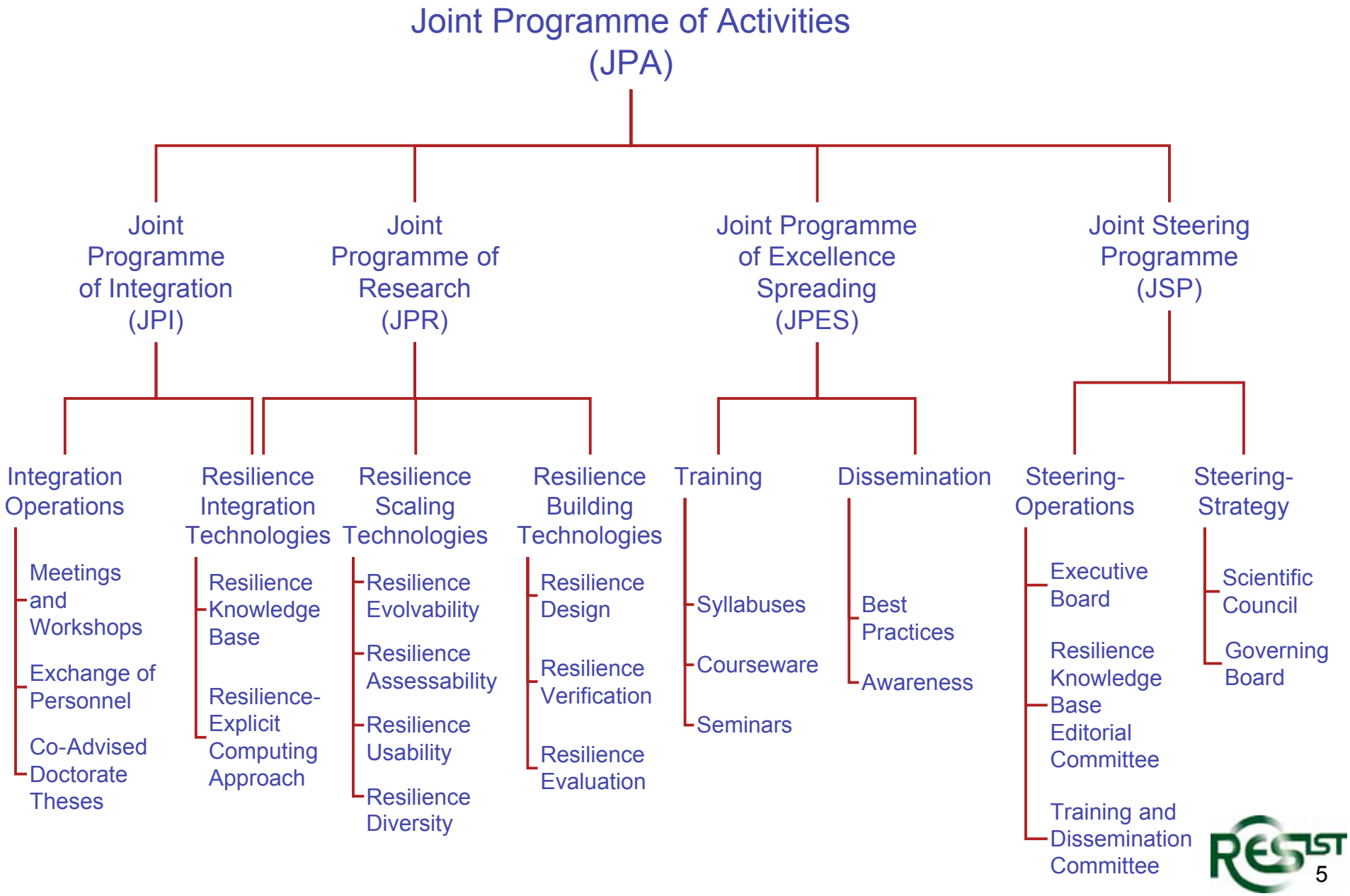

(Reasonably) known: High dependability
for safety-critical or availability-critical systems
Avionics, railway signalling,
nuclear control, etc.
Transaction processing,
back-end servers, etc.
Continuous complexity growth
Large, networked, evolving, applications running on open systems, fixed or mobile,
i.e., ubiquitous systems
Dependability gap between necessary trust for realistic AmI and operational statistics
Scalability of Dependability
In addition to rigorous functional design, provision of
Resilience for Survivability
Development or
physical
accidental faults
Malicious
attacks
Interaction
mistakes
Vulnerabilities


Changes
Functional changes
Environmental changes
Technological changes
Dependability scalability
Dependability Scalability Properties
Dependability Extensibility
Dependability Composability
Dependability Adaptivity
Dependability Consistency
Resilience Scaling Technologies
Resilience Evolvability
Resilience Assessability
Resilience Usability
Resilience Diversity
Resilience Building Technologies
Resilience Design
Resilience Verification
Resilience Evaluation

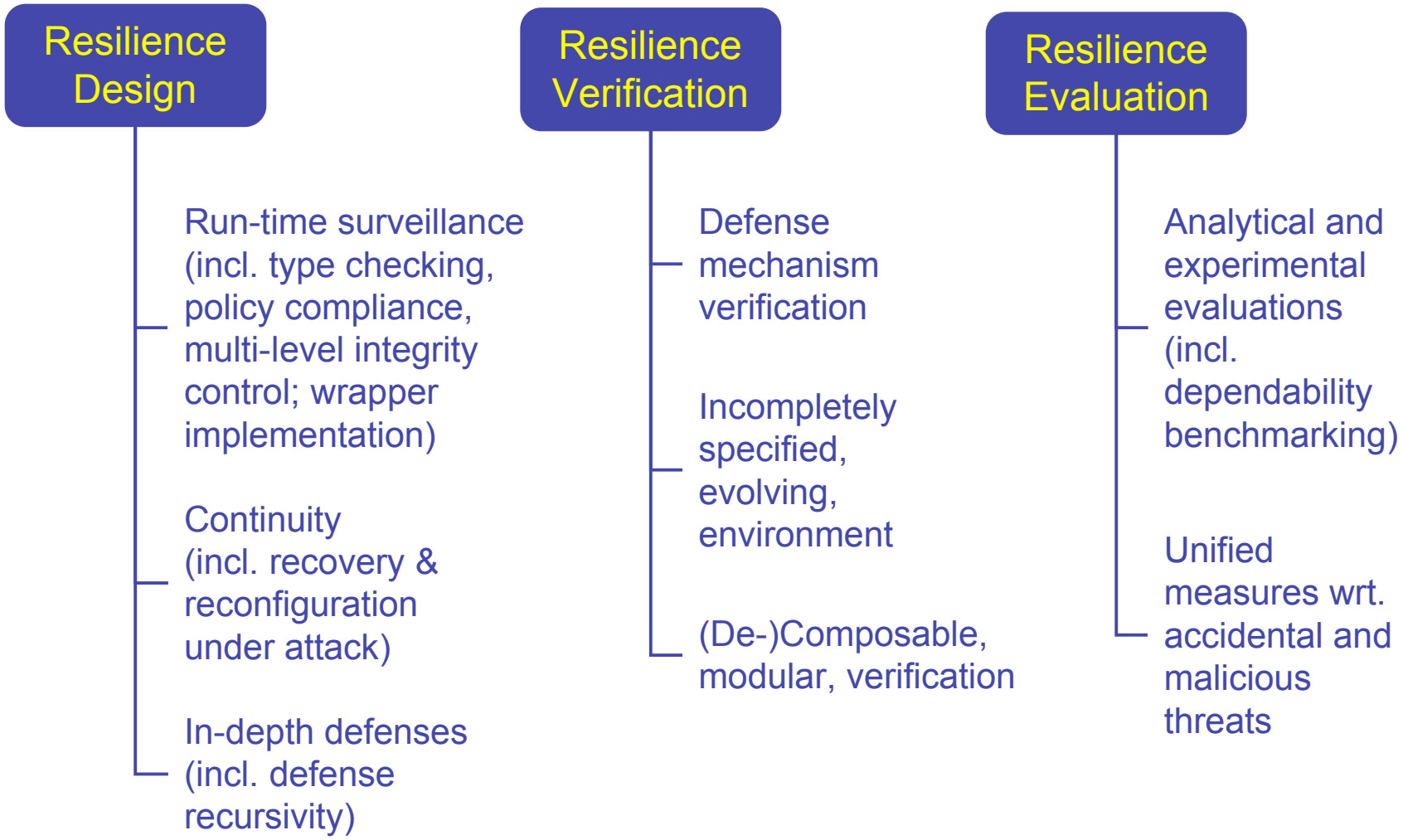
Logic


Joint Programme of Activities
Joint Programme of Integration (JPI)
Joint Programme of Research (JPR)
Joint Programme of Excellence Spreading (JPES)
Joint Steering Programme (JSP)
Integration Operations
Resilience Integration Technologies
Resilience Scaling Technologies
Resilience Building Technologies
Training
Dissemination
Steering-Operations
Steering-Strategy
Resilience Building Technologies
Design
Verification
Evaluation
Resilience Scaling Technologies
Evolvability
Assessability
Usability
Diversity
Resilience Integration Technologies
Resilience Knowledge Base
Resilience-Explicit Computing

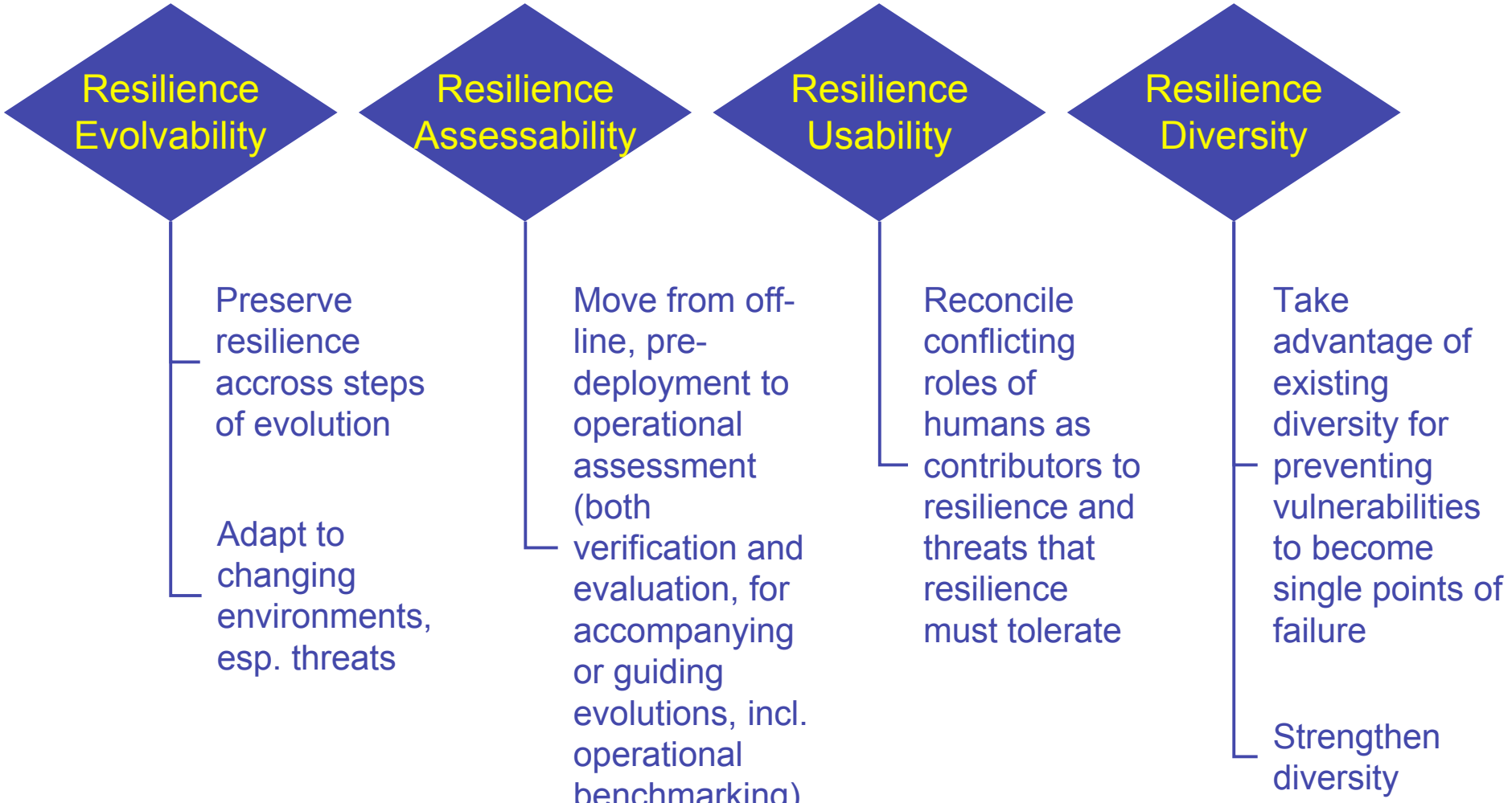
Joint Programme of Activities insight



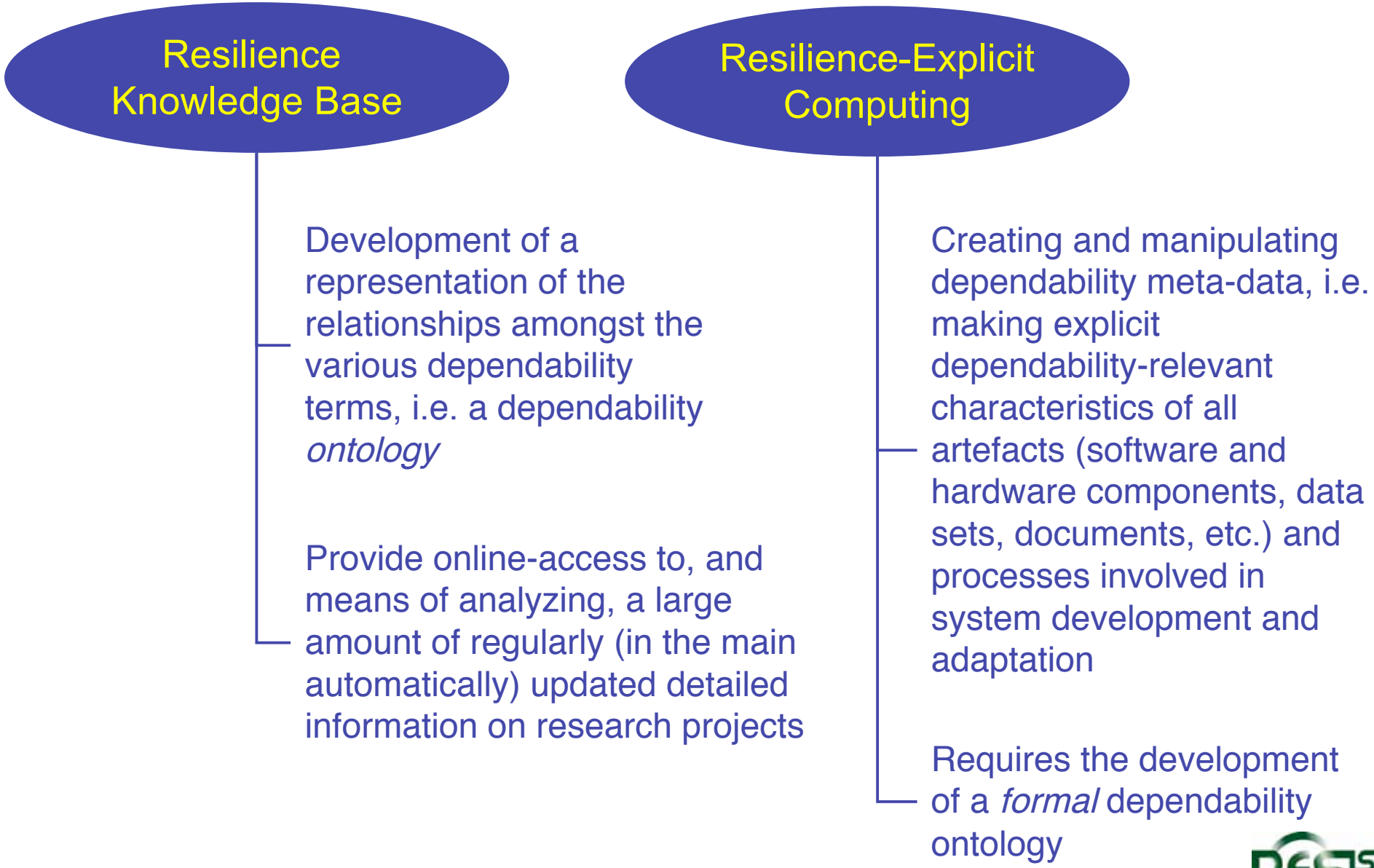
Resilience Building Technologies



Resilience Scaling Technologies



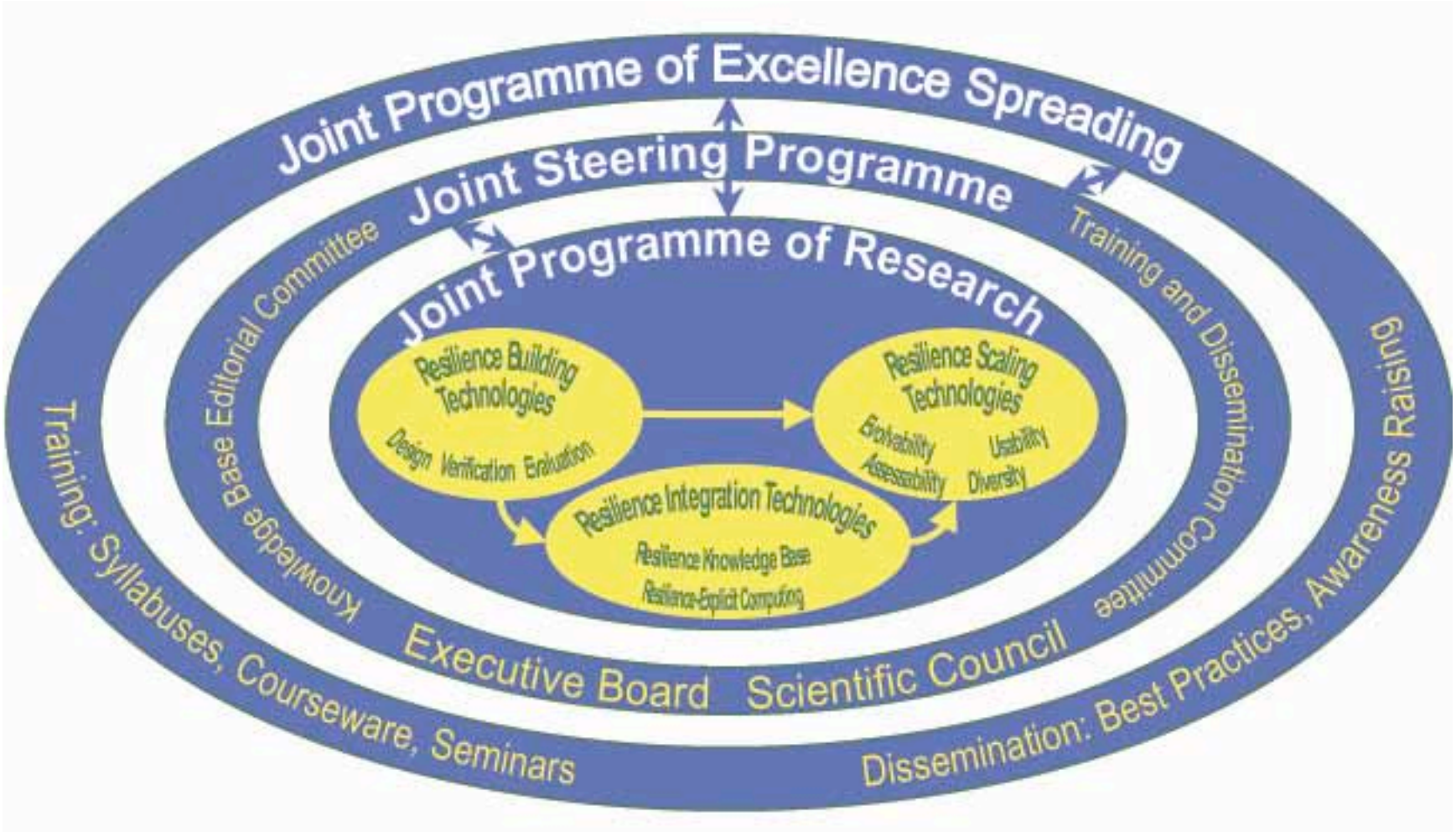
Resilience Integration Technologies



Partnership

	Expertise				Country	Academia (Ac) / Industry (Ind)
	Threat resilience: development or physical Accidental faults (A) / Malicious attacks (M) / Interaction mistakes (I)			Mobile computing		
	A	M	I			
LAAS-CNRS [coordinator]	X	X		X	FR	Ac
Budapest U.	X				HU	Ac
City U., London	X	X	X		UK	Ac
Darmstadt U.	X	X			DE	Ac
Deep Blue			X		IT	Ind - SME
Eurecom		X		X	FR	Ac
France Telecom R&D	X	X		X	FR	Ind
IBM Research Zurich		X			CH	Ind
IRISA	X			X	FR	Ac
IRIT			X		FR	Ac
Vytautas Magnus U., Kaunas	X				LT	Ac
Lisbon U.	X	X		X	PT	Ac
Newcastle U.	X	X	X		UK	Ac
Pisa U.	X	X	X		IT	Ac
QinetiQ	X	X			UK	Ind
Roma-La Sapienza U.	X			X	IT	Ac
Ulm U.	X				DE	Ac
Southampton U.	Resilience Knowedge Base building				UK	Ac

71 researchers plus 44 students, 3 year duration

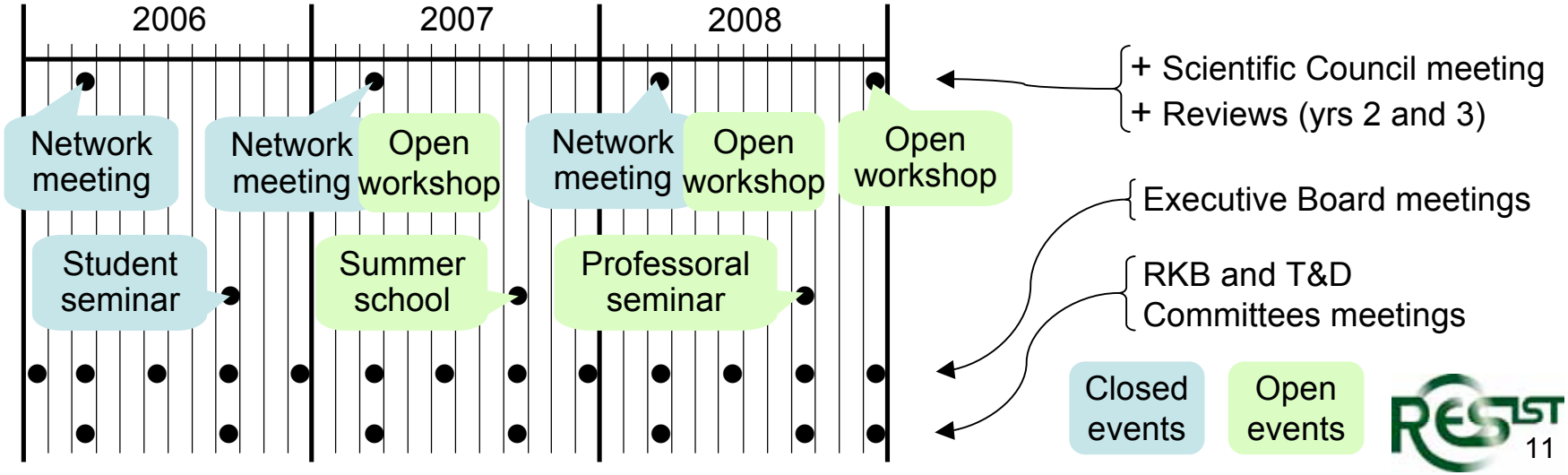


Scalably resilient policies, algorithms and mechanisms for ubiquitous computing systems

Organisation

☞ Composition – Multidisciplinarity for holistic approach

Partners' expertise — Threat Resilience		
Accidental faults	Malicious attacks	Interaction mistakes
13 [Ac: 11, Ind: 2]	10 [Ac: 7, Ind: 3]	5 [Ac: 4, Ind: 1]

☞ Management

☞ Event Schedule