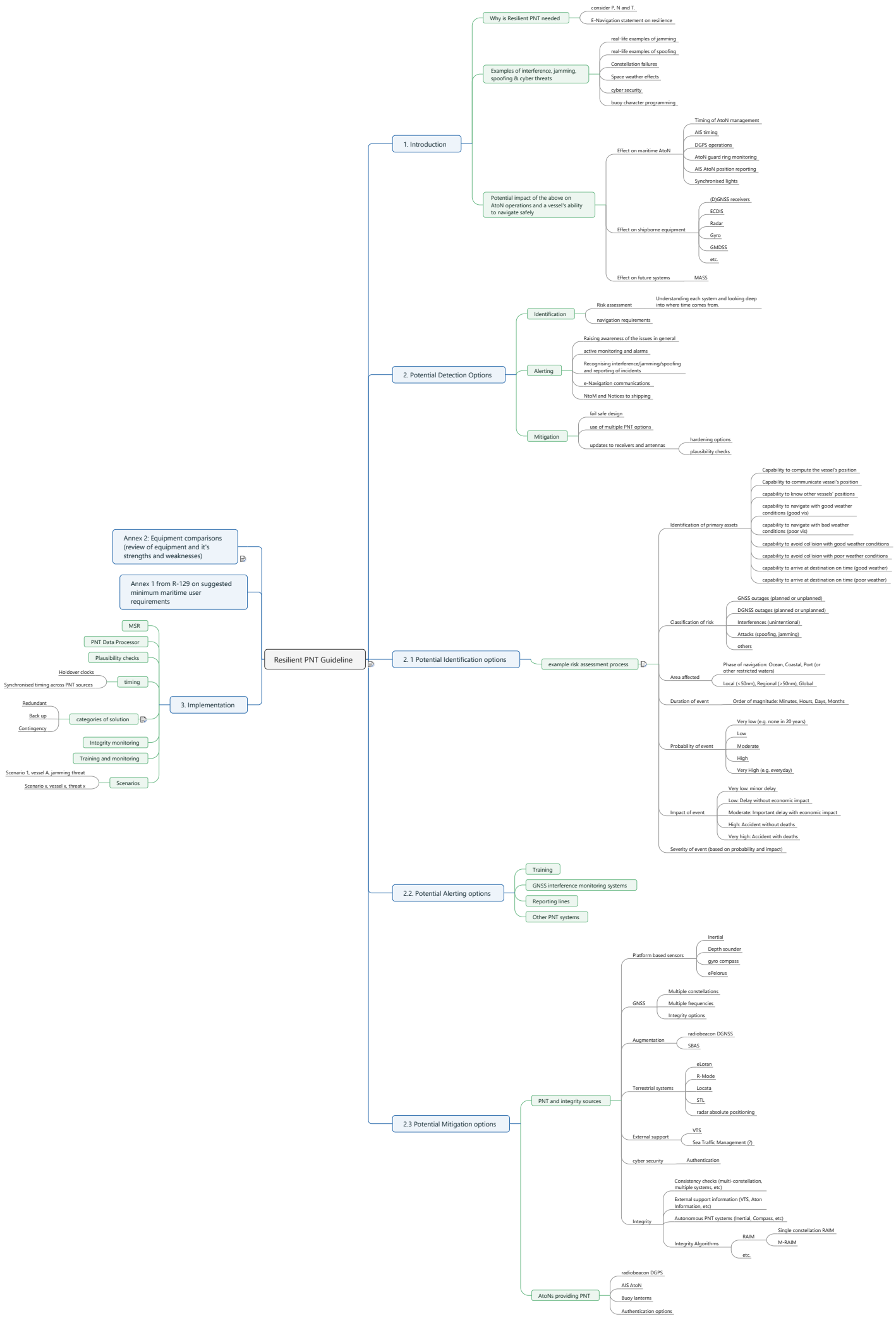
Resilient PNT Guideline
1. Introduction
Why is Resilient PNT needed
consider P, N and T.
E-Navigation statement on resilience
Examples of interference, jamming, spoofing & cyber threats
real-life examples of jamming
real-life examples of spoofing
Constellation failures
Space weather effects
cyber security
buoy character programming
Potential impact of the above on AtoN operations and a vessel's ability to navigate safely
Effect on maritime AtoN
Timing of AtoN management
AIS timing
DGPS operations
AtoN guard ring monitoring
AIS AtoN position reporting
Synchronised lights
Effect on shipborne equipment
(D)GNSS receivers
ECDIS
Radar
Gyro
GMDSS
etc.
Effect on future systems
MASS
2. Potential Detection Options
Identification
Risk assessment
Understanding each system and looking deep into where time comes from.
navigation requirements
Alerting
Raising awareness of the issues in general
active monitoring and alarms
Recognising interference/jamming/spoofing and reporting of incidents
e-Navigation communications
NtoM and Notices to shipping
Mitigation
fail safe design
use of multiple PNT options
updates to receivers and antennas
hardening options
plausibility checks
2. 1 Potential Identification options
example risk assessment process
Identification of primary assets
Capability to compute the vessel's position
Capability to communicate vessel's position
capability to know other vessels' positions
capability to navigate with good weather conditions (good vis)
capability to navigate with bad weather conditions (poor vis)
capability to avoid collision with good weather conditions
capability to avoid collision with poor weather conditions
capability to arrive at destination on time (good weather)
capability to arrive at destination on time (poor weather)
Classification of risk
GNSS outages (planned or unplanned)
DGNSS outages (planned or unplanned)
Interferences (unintentional)
Attacks (spoofing, jamming)
others
Area affected
Phase of navigation: Ocean, Coastal, Port (or other restricted waters)
Local (<50nm), Regional (>50nm), Global
Duration of event
Order of magnitude: Minutes, Hours, Days, Months
Probability of event
Very low (e.g. none in 20 years)
Low
Moderate
High
Very High (e.g. everyday)
Impact of event
Very low: minor delay
Low: Delay without economic impact
Moderate: Important delay with economic impact
High: Accident without deaths
Very high: Accident with deaths
Severity of event (based on probability and impact)
2.2. Potential Alerting options
Training
GNSS interference monitoring systems
Reporting lines
Other PNT systems
2.3 Potential Mitigation options
PNT and integrity sources
Platform based sensors
Inertial
Depth sounder
gyro compass
ePelorus
GNSS
Multiple constellations
Multiple frequencies
Integrity options
Augmentation
radiobeacon DGNSS
SBAS
Terrestrial systems
eLoran
R-Mode
Locata
STL
radar absolute positioning
External support
VTS
Sea Traffic Management (?)
cyber security
Authentication
Integrity
Consistency checks (multi-constellation, multiple systems, etc)
External support information (VTS, Aton Information, etc)
Autonomous PNT systems (Inertial, Compass, etc)
Integrity Algorithms
RAIM
Single constellation RAIM
M-RAIM
etc.
AtoNs providing PNT
radiobeacon DGPS
AIS AtoN
Buoy lanterns
Authentication options
3. Implementation
MSR
PNT Data Processor
Plausibility checks
timing
Holdover clocks
Synchronised timing across PNT sources
categories of solution
Redundant
Back up
Contingency
Integrity monitoring
Training and monitoring
Scenarios
Scenario 1, vessel A, jamming threat
Scenario x, vessel x, threat x
Annex 2: Equipment comparisons (review of equipment and it's strengths and weaknesses)
Annex 1 from R-129 on suggested minimum maritime user requirements