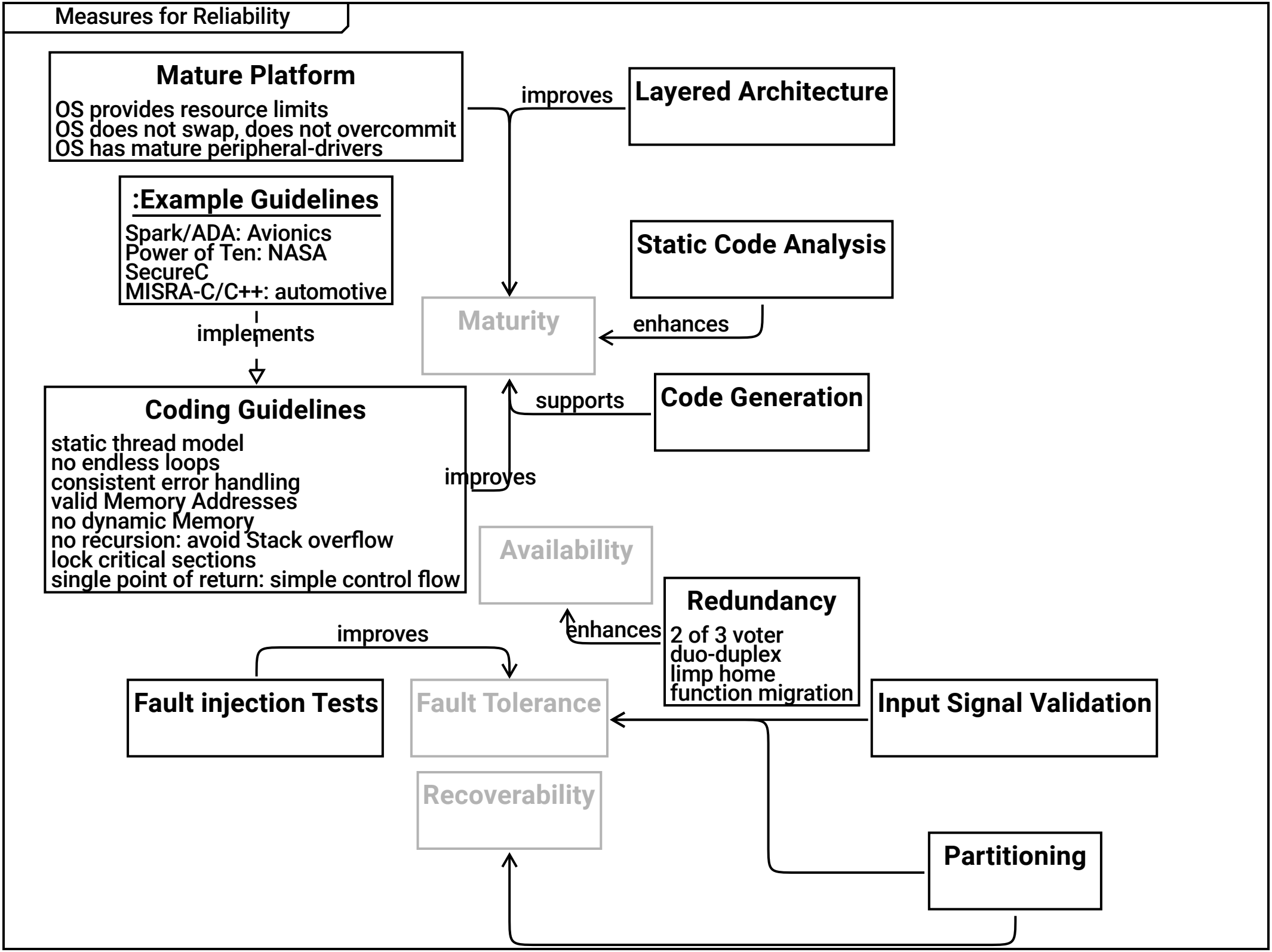
Measures for Reliability
Mature Platform
OS provides resource limits
OS does not swap, does not overcommit
OS has mature peripheral-drivers
improves
Layered Architecture
:Example Guidelines
Spark/ADA: Avionics
Power of Ten: NASA
SecureC
MISRA-C/C++: automotive
implements
Static Code Analysis
Maturity
enhances
supports
Code Generation
Coding Guidelines
static thread model
no endless loops
consistent error handling
valid Memory Addresses
no dynamic Memory
no recursion: avoid Stack overflow
lock critical sections
single point of return: simple control flow
improves
Availability
Redundancy
2 of 3 voter
duo-duplex
limp home
function migration
enhances
improves
Fault injection Tests
Fault Tolerance
Input Signal Validation
Recoverability
Partitioning