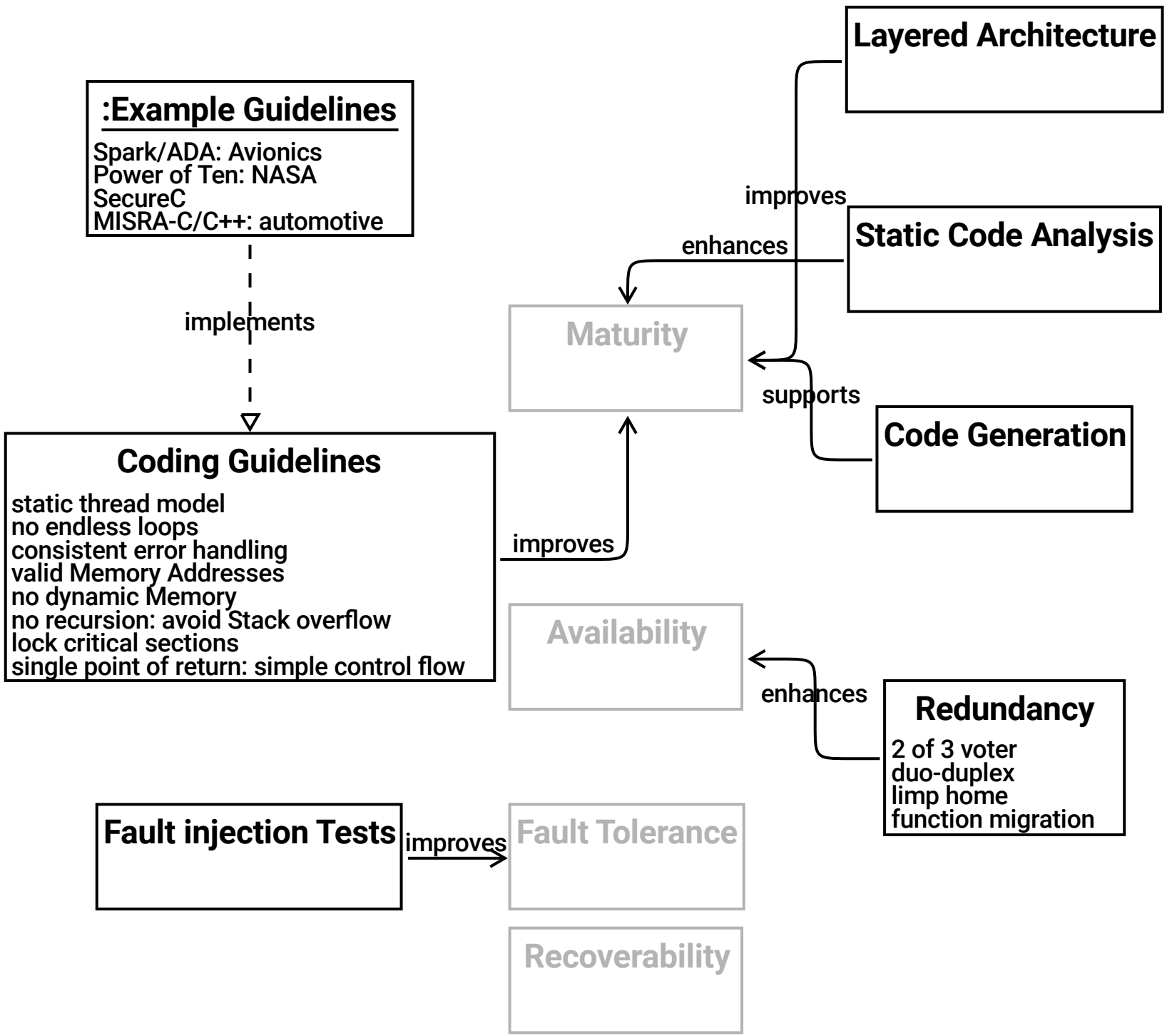
Layered Architecture
:Example Guidelines
Spark/ADA: Avionics
Power of Ten: NASA
SecureC
MISRA-C/C++: automotive
improves
Static Code Analysis
enhances
implements
Maturity
supports
Code Generation
Coding Guidelines
static thread model
no endless loops
consistent error handling
valid Memory Addresses
no dynamic Memory
no recursion: avoid Stack overflow
lock critical sections
single point of return: simple control flow
improves
Availability
enhances
Redundancy
2 of 3 voter
duo-duplex
limp home
function migration
Fault injection Tests
improves
Fault Tolerance
Recoverability