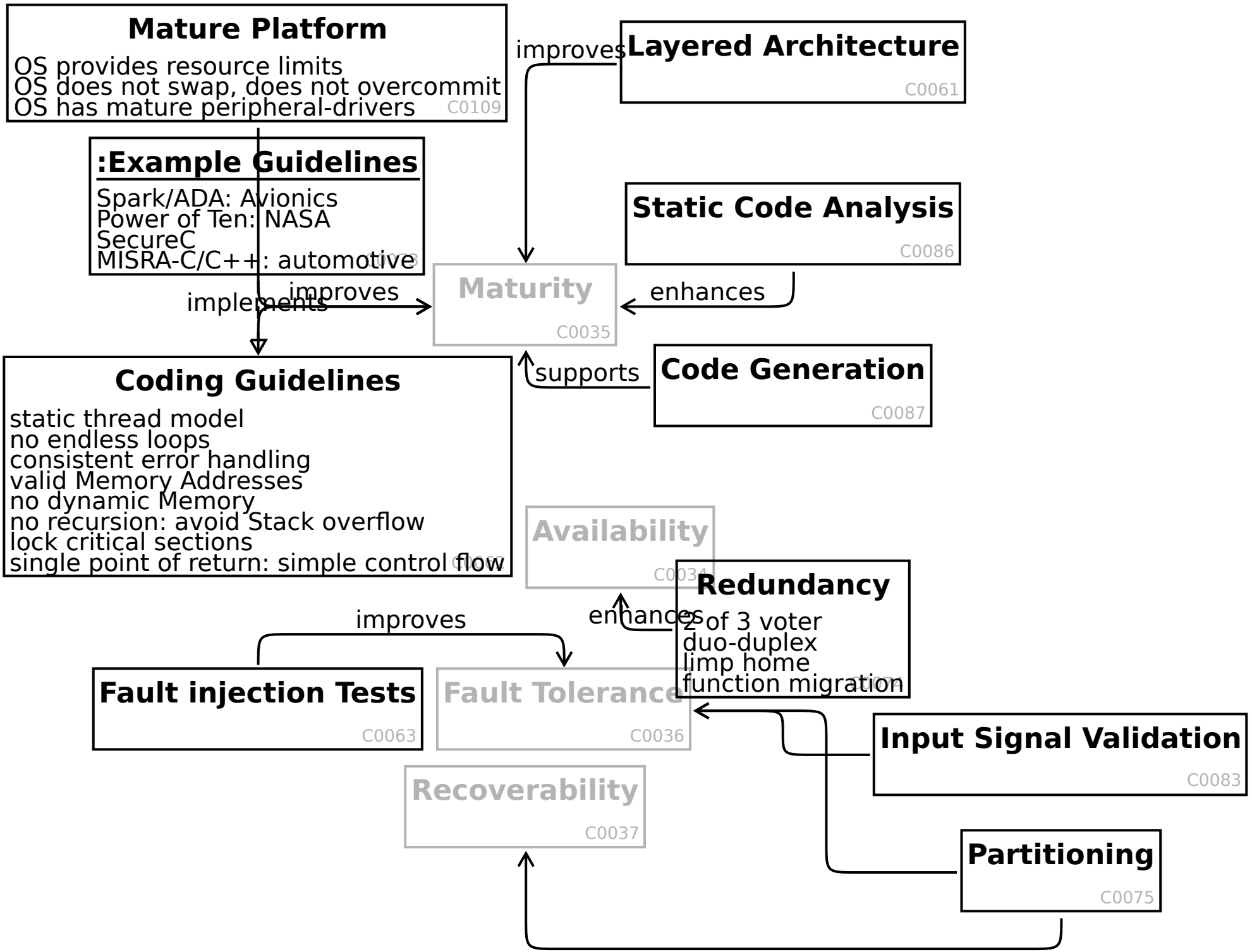
Mature Platform
OS provides resource limits
OS does not swap, does not overcommit
OS has mature peripheral-drivers
C0109
improves
Layered Architecture
C0061
:Example Guidelines
Spark/ADA: Avionics
Power of Ten: NASA
SecureC
MISRA-C/C++: automotive
C0088
Static Code Analysis
C0086
improves
implements
Maturity
C0035
enhances
supports
Code Generation
C0087
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
C0062
Availability
C0034
Redundancy
2 of 3 voter
duo-duplex
limp home
function migration
C0041
improves
enhances
Fault injection Tests
C0063
Fault Tolerance
C0036
Input Signal Validation
C0083
Recoverability
C0037
Partitioning
C0075