

:Example Guidelines

Spark/ADA: Avionics
Power of Ten: NASA
SecureC
MISRA-C/C++: automotive

implements



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

Layered Architecture

improves

improves

Maturity

Availability

enhances

Fault Tolerance

improves

Recoverability

Redundancy

2 of 3 voter
duo-duplex
limp home
function migration

Fault injection Tests