

: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

Fault injection Tests

improves

Fault Tolerance

Recoverability

Availability

improves

Maturity

enhances

improves

supports

Layered Architecture

Static Code Analysis

Code Generation

enhances

Redundancy

2 of 3 voter
duo-duplex
limp home
function migration