

Measures for Reliability

Mature Platform

OS provides resource limits
OS does not swap, does not overcommit
OS has mature peripheral-drivers

:Example Guidelines

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

Layered Architecture

Static Code Analysis

Code Generation

Redundancy

2 of 3 voter
duo-duplex
limp home
function migration

Input Signal Validation

Partitioning

Maturity

Availability

Fault Tolerance

Recoverability

Fault injection Tests

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

enhances

supports

improves

enhances

improves

implements

