

**Mature Platform**

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

C0109

**: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

improves

**Fault injection Tests**

C0063

**Fault Tolerance**

C0036

**Recoverability**

C0037

improves

**Layered Architecture**

C0061

**Static Code Analysis**

C0086

enhances

**Maturity**

C0035

supports

**Code Generation**

C0087

improves

**Availability**

C0034

enhances

**Redundancy**

2 of 3 voter  
duo-duplex  
limp home  
function migration

**Input Signal Validation**

C0083

**Partitioning**

C0075