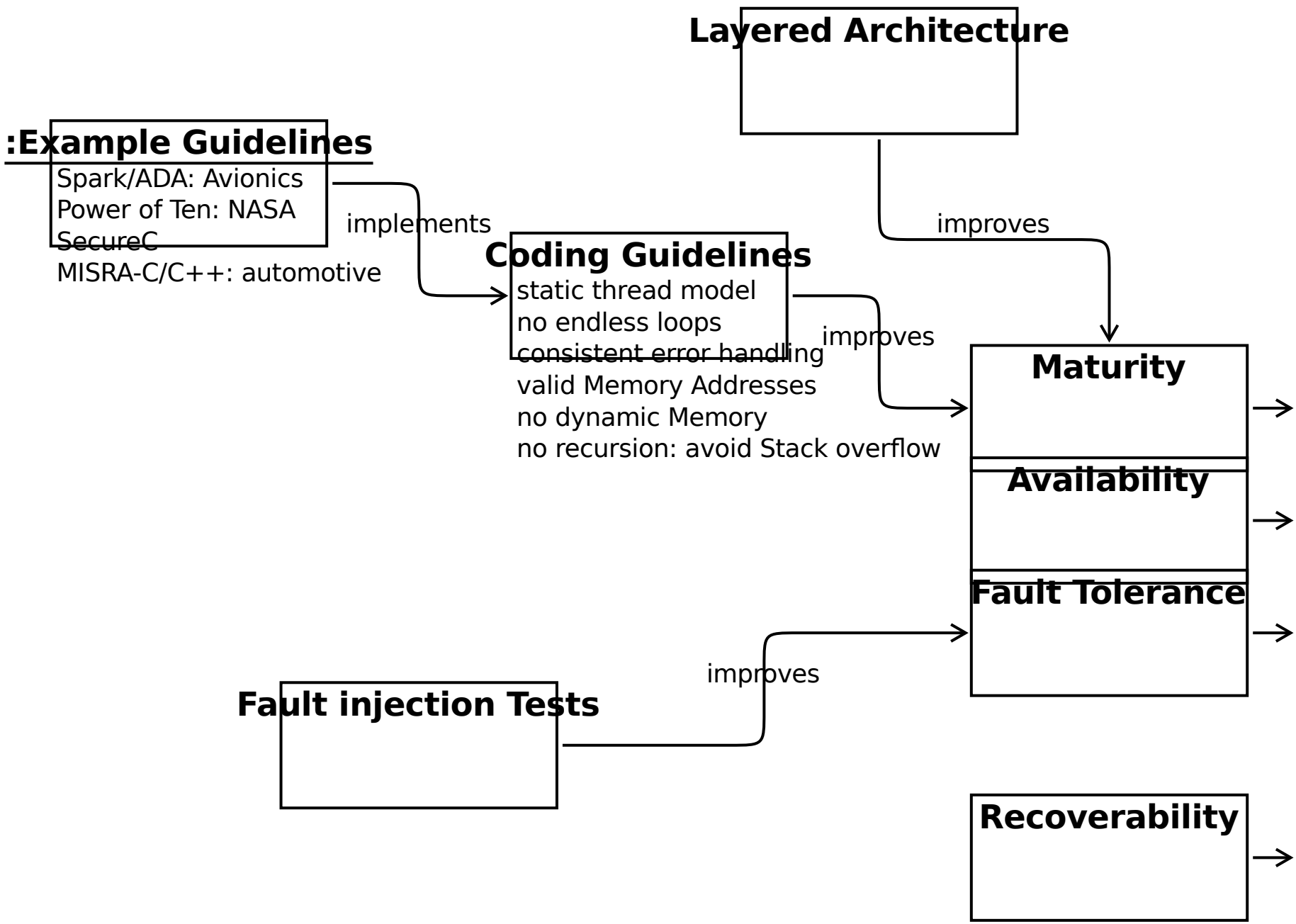
Layered Architecture
:Example Guidelines
Spark/ADA: Avionics
Power of Ten: NASA
SecureC
MISRA-C/C++: automotive
implements
Coding Guidelines
static thread model
no endless loops
consistent error handling
valid Memory Addresses
no dynamic Memory
no recursion: avoid Stack overflow
improves
improves
Maturity
Availability
Fault Tolerance
improves
Fault injection Tests
Recoverability