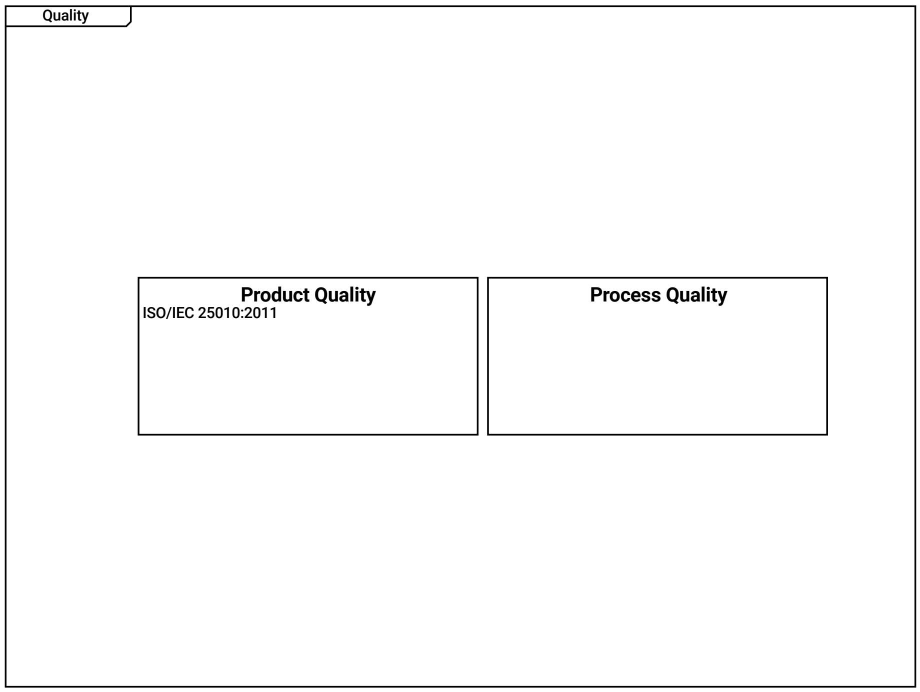
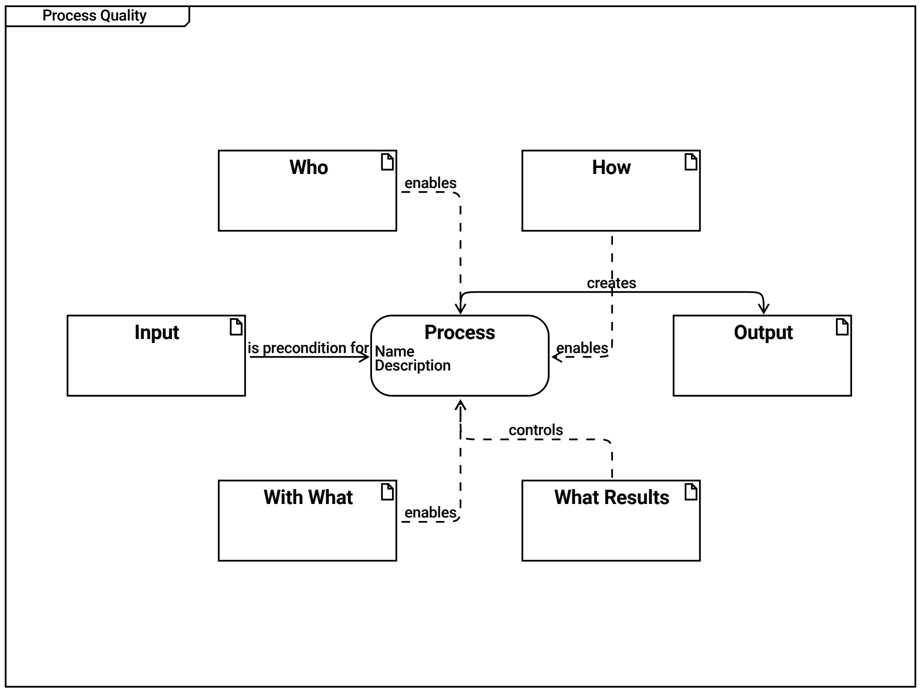
1 Quality Example



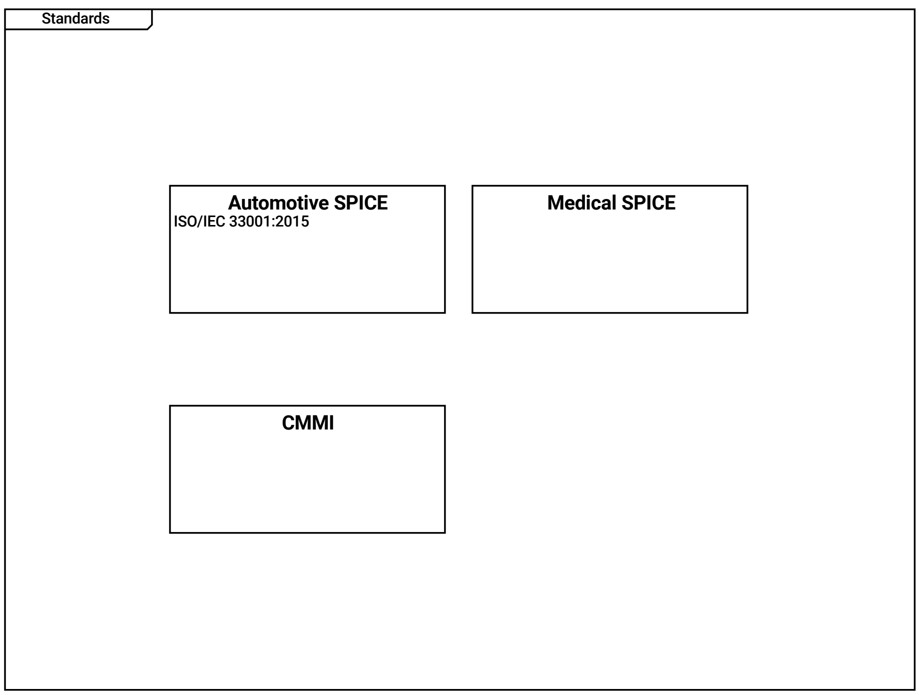

```
Quality


Product Quality
  ISO/IEC 25010:2011


Process Quality
```

2 Process Quality




```
Process Quality
| The turtle diagram shows the elements of a process.


Who
| Roles,
| Skills, Knowledge,
| Trainings
  enables --> Process


How
| Guidelines, Checklists,
| Templates
  enables --> Process


Input
  is precondition for --> Process
```

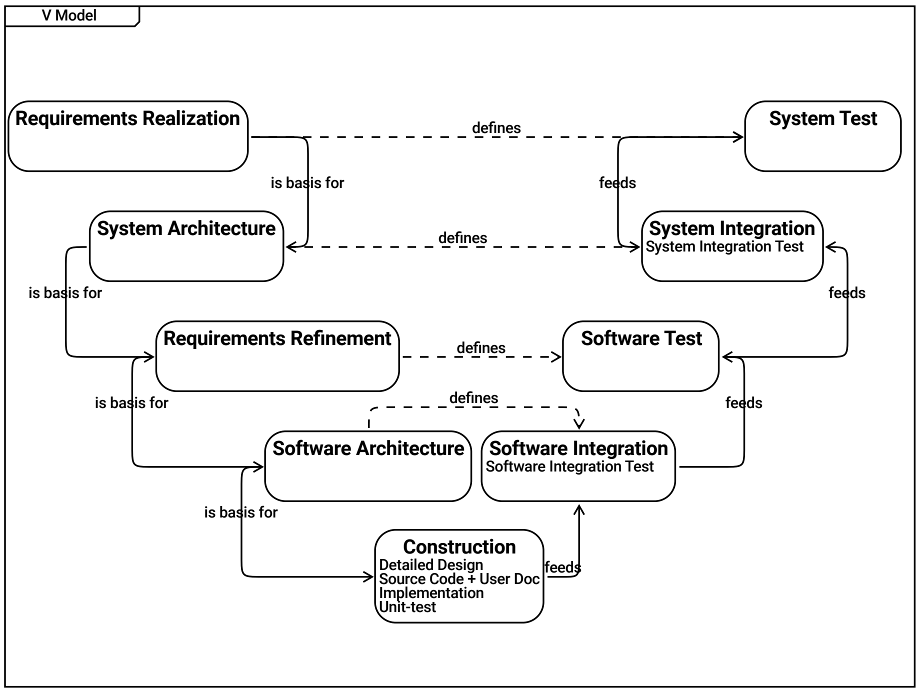
```
Process
  Name
  Description
  creates --> Output


Output
| Process output,
| Evidence on performed process


With What
  enables --> Process


What Results
  controls --> Process
```




```
Standards


Automotive SPICE
  ISO/IEC 33001:2015
```

Medical SPICE

CMMI



V Model

Requirements Realization
  is basis for --> System Architecture
  defines --> System Test

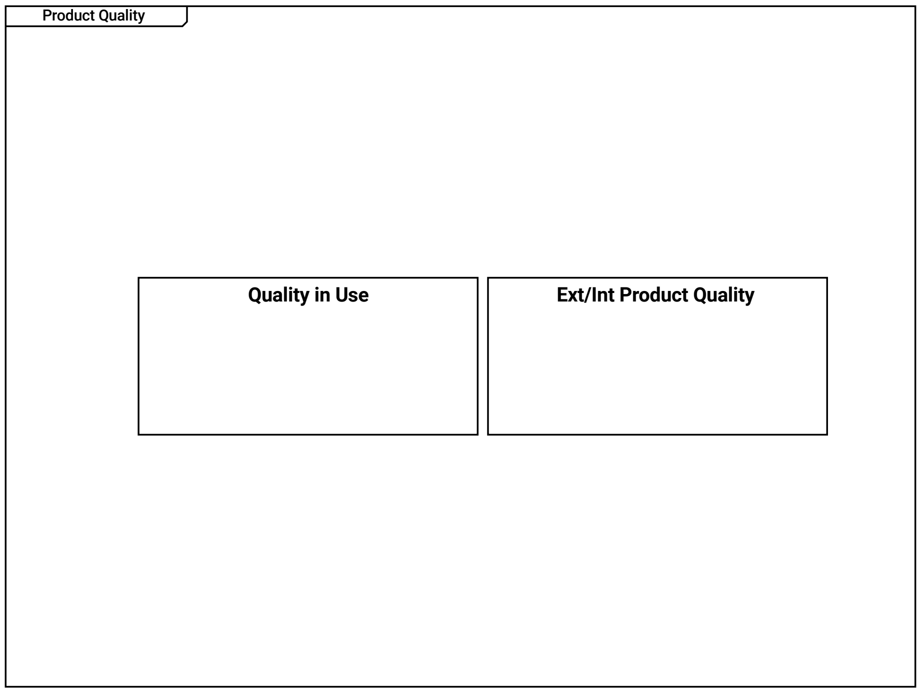
System Test

System Architecture
  is basis for --> Requirements Refinement
  defines --> System Integration

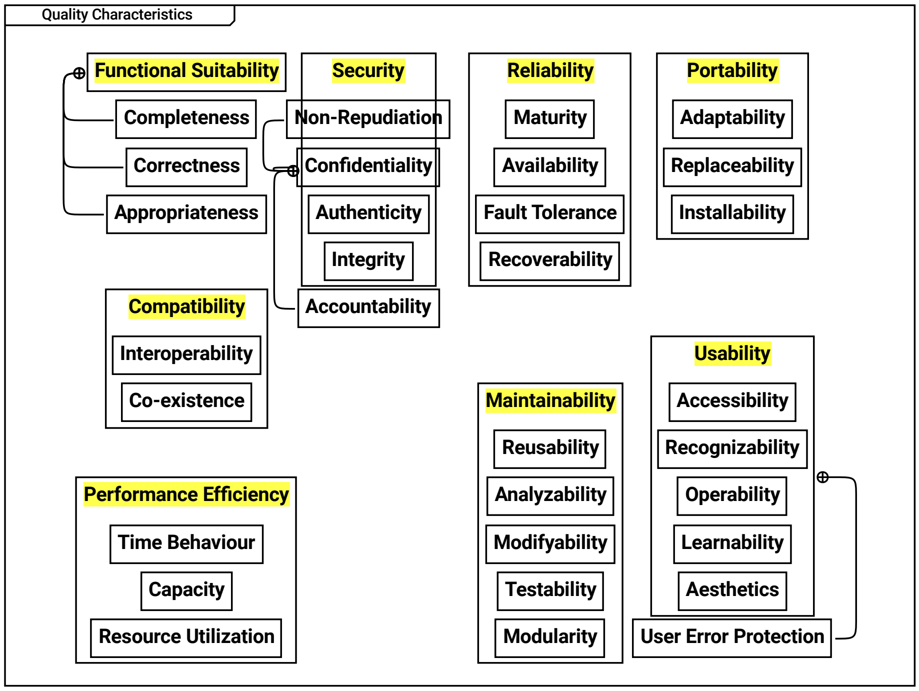
System Integration
  System Integration Test

```
  feeds --> System Test


Requirements Refinement
  is basis for --> Software Architecture
  defines --> Software Test


Software Test
  feeds --> System Integration


Software Architecture
  defines --> Software Integration
  is basis for --> Construction


Software Integration
  Software Integration Test
  feeds --> Software Test


Construction
  Detailed Design
  Source Code + User Doc
  Implementation
  Unit-test
  feeds --> Software Integration
```

3 Product Quality




```
Product Quality


Quality in Use
| Quality in use can be measured when the product is already in use,
| e.g. the percentage of satisfied customers can be determined.


Ext/Int Product Quality
| Product quality are internal and externally visible qualities,
| such as memory consumption or startup timings.
```




```
Quality Characteristics
| according to ISO 25010


Functional Suitability
   --> Completeness
   --> Correctness
   --> Appropriateness


Security
   --> Authenticity
   --> Non-Repudiation
   --> Accountability
   --> Integrity
   --> Confidentiality


Reliability
   --> Maturity
   --> Availability
   --> Fault Tolerance
   --> Recoverability
```

```
Portability
   --> Adaptability
   --> Installability
   --> Replaceability


Completeness


Non-Repudiation


Maturity


Adaptability


Correctness


Confidentiality


Availability


Replaceability


Appropriateness


Authenticity


Fault Tolerance


Installability


Integrity
```

```
Recoverability


Compatibility
   --> Co-existence
   --> Interoperability


Accountability


Interoperability


Usability
   --> Recognizability
   --> Learnability
   --> Operability
   --> User Error Protection
   --> Aesthetics
   --> Accessibility


Co-existence


Maintainability
   --> Testability
   --> Modifyability
   --> Analyzability
   --> Reusability
   --> Modularity


Accessibility


Reusability


Recognizability


Performance Efficiency
   --> Time Behaviour
```

--> Resource Utilization
--> Capacity

Analyzability

Operability

Time Behaviour

Modifyability

Learnability

Capacity

Testability

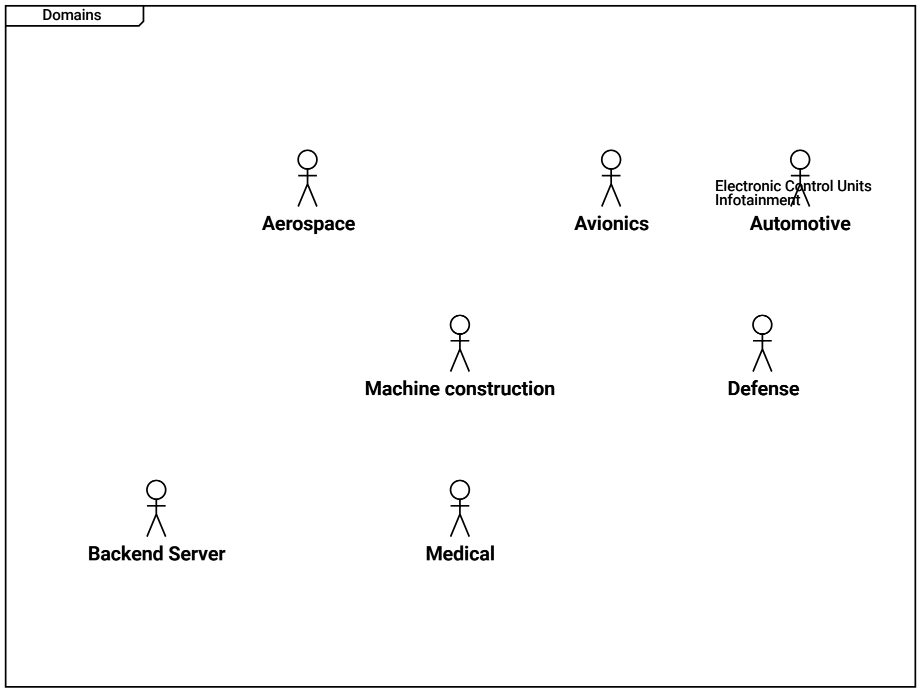
Aesthetics

Resource Utilization

Modularity

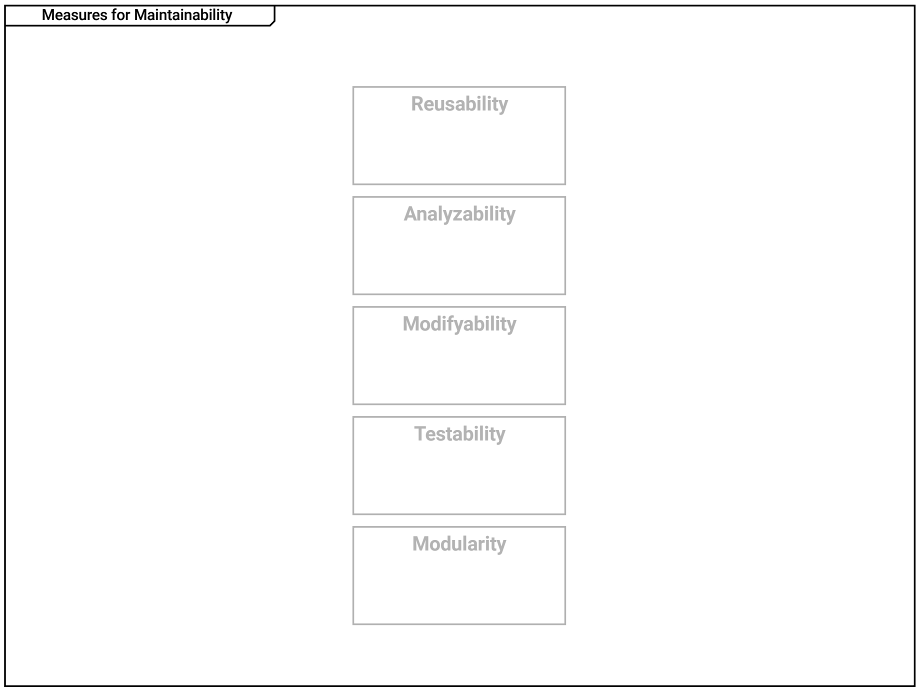
User Error Protection

3.1 Product Quality Measures




```
Domains


Aerospace


Avionics


Automotive
  Electronic Control Units
  Infotainment


Machine construction


Defense


Backend Server
```

Medical



Measures for Maintainability

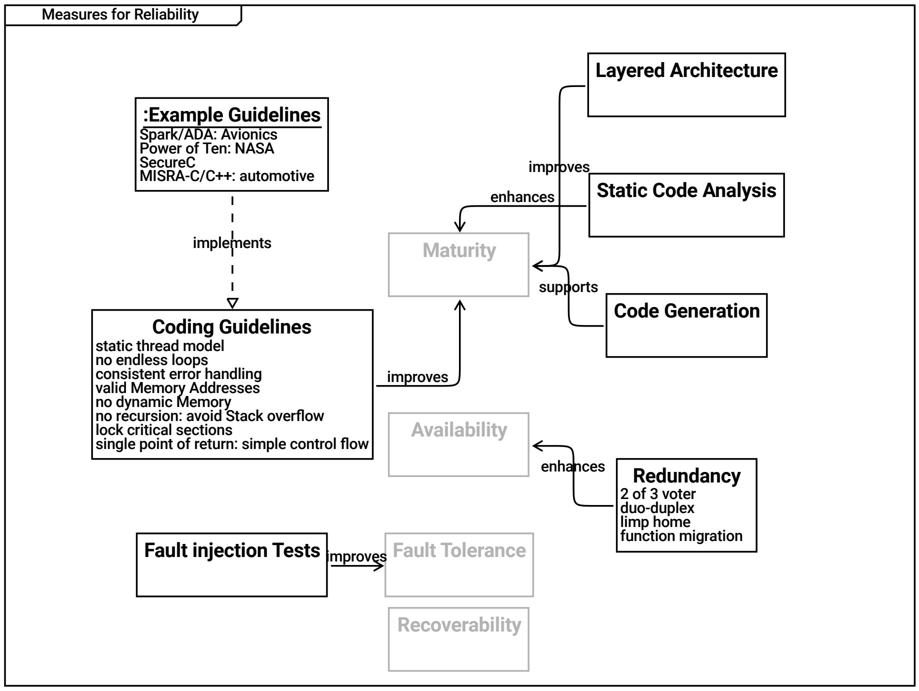
Reusability

Analyzability

Modifyability

Testability

Modularity

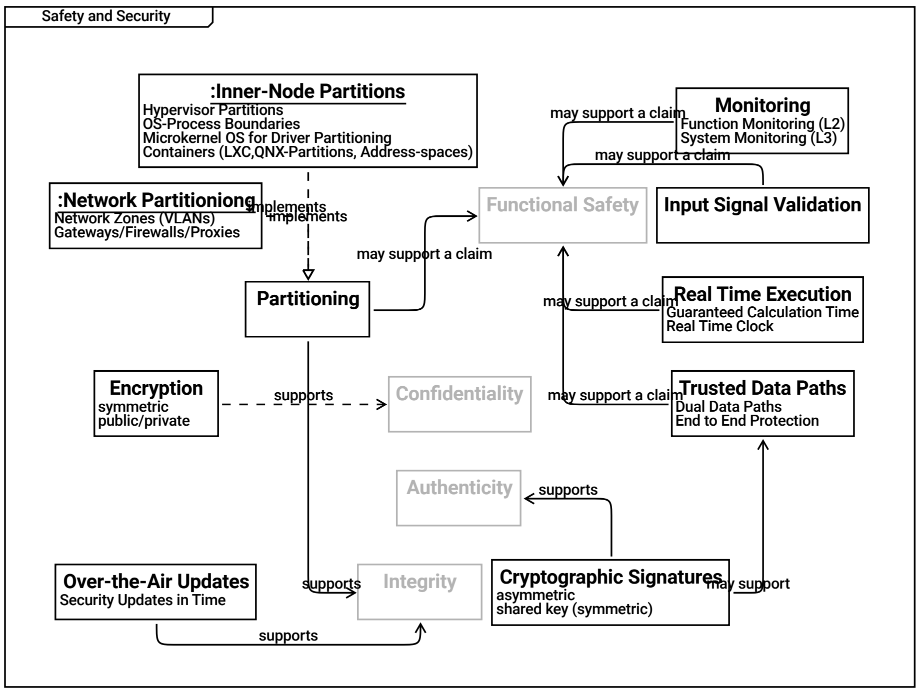



```
Measures for Reliability


Layered Architecture
  improves --> Maturity


Example Guidelines
  Spark/ADA: Avionics
  Power of Ten: NASA
  SecureC
  MISRA-C/C++: automotive
  implements --> Coding Guidelines


Static Code Analysis
  enhances --> Maturity


Maturity


Code Generation
```

```
| An understandable model and a small code generator
| allow to generate mature software.
  supports --> Maturity


Coding Guidelines
  static thread model
  | Execution threads shall not be started/stopped dynamically
  no endless loops
  | Every loop shall have a counter to ensures that
  | after a predefined maximum value the loop is definitely quit
  consistent error handling
  | Inconsistencies in error handling make
  | bugs in error handling more likely
  valid Memory Addresses
  | Only valid memory addresses may be read/written.
  | E.g. Java solves this by prohibiting pointers,
  | In C/C++, check pointers and array indices before usage
  no dynamic Memory
  | When the program is running,
  | - it must not fail due to
  |   - memory fragmentation (virtual addresses/physical pages)
  |   - out of memory situations
  | - it shall have a defined timing (which new/malloc cannot provide)
  no recursion: avoid Stack overflow
  lock critical sections
  | Always lock critical sections.
  | Exceptions to locking are a nightmare.
  single point of return: simple control flow
  | Simple control flow is key to understandable code
  improves --> Maturity


Availability


Redundancy
  2 of 3 voter
  duo-duplex
  limp home
  function migration
  enhances --> Availability


Fault injection Tests
  improves --> Fault Tolerance
```

Fault Tolerance

Recoverability



Safety and Security
| Functional safety and security are different goals
| but have common mechanisms to support these.
|
| The diagram is not meant to be complete,
| it just shows that technical mechanisms support quality goals.

Inner-Node Partitions
  Hypervisor Partitions
  OS-Process Boundaries
  Microkernel OS for Driver Partitioning
  Containers (LXC,QNX-Partitions, Address-spaces)
  implements --> Partitioning

Monitoring

```
  Function Monitoring (L2)
  System Monitoring (L3)
  may support a claim --> Functional Safety


Network Partitioniong
  Network Zones (VLANs)
  Gateways/Firewalls/Proxies
  implements --> Partitioning


Functional Safety


Input Signal Validation
  may support a claim --> Functional Safety


Partitioning
  supports --> Integrity
  may support a claim --> Functional Safety


Real Time Execution
  Guaranteed Calculation Time
  Real Time Clock
  may support a claim --> Functional Safety


Encryption
  symmetric
  public/private
  supports --> Confidentiality


Confidentiality


Trusted Data Paths
  Dual Data Paths
  End to End Protection
  may support a claim --> Functional Safety


Authenticity
```

```
Over-the-Air Updates
  Security Updates in Time
  supports --> Integrity


Integrity


Cryptographic Signatures
  asymmetric
  shared key (symmetric)
  supports --> Authenticity
  may support --> Trusted Data Paths
```