**NASPInet 2.0 Architectural Specifications and Guidance**

Draft ToC v 0.2

4 May 2017

1. **Background and Purpose**  
   1.1 Short history of original NASPINet specs and ARRA experience;   
   (reference the analysis report from NASPInet 2.0 project and cite some key results)

1.2 Discussion of justification for a new specification.

1. **Scope**  
   initial broad scope statement  
   overview of applications/use cases, present and forward-looking; include wide area closed loop protection and control, adaptive protection, etc.  
   cite previous application lists; add necessary forward leaning cases
2. **Key Architectural Principles**  
   3.1 basic good network practices (core and edge model; layering, etc.)  
   3.2 use of international open standards  
   3.3 function allocation concepts & good practice (network vs. middleware vs. application)  
   3.4 some implications of these principles:   
    avoid PDC stacking  
    minimize use of protocol conversion gateways, etc.
3. **Core Requirements**  
   scalability latency minimization reliability/(min packet loss) cybersecurity  
   performance functional flexibility data persistence open standards usage/conformance data sharing data rates availability extensibility service classes
4. **Problem Domain Reference Model**  
   5.1 emerging trends & systemic issues; regulatory/public policy issues  
   5.2 key constraints & barriers (example: geographic constraints)  
   5.3 entity-relationship (industry structure) model(s)  
   5.4 logical/data flow model(s)
5. **Architectural Specifications and Recommendations**  
   6.1 function class definitions (capabilities)  
   6.2 component class definitions (devices and systems)   
   6.3 networks  
    6.3.1 structures/topologies (intra-utility, WAN)  
    6.3.2 protocols, operating modes  
    6.3.3 network provisioning/monitoring/management: AAA[[1]](#footnote-1); ZTD[[2]](#footnote-2), FCAPS[[3]](#footnote-3)  
    6.3.4 QoS management  
    6.3.5 timing distribution   
    6.3.6 network level cyber security  
   6.4 systems  
    6.4.1 function allocation(s) – data acquisition/data transfer modes, synchronization,   
    data management (persistence and curation),   
    event processing, analysis/visualization, registry services,   
    name/directory services, access control/access methods, device   
    provisioning/configuration, system administration, event logging,  
    failure mode management, etc.  
    6.4.2 system structures and interfaces  
    6.4.3 system level cyber security  
   6.5 standards  
    IEEE C37.118, IEC 61850-90-5, IP protocol suite, IEEE 1588 (timing),   
    IEEE 1451 (smart transducers),   
    IEC 61968/61970 (CIM), IEC 27040 (storage security),   
    IEEE P1619 (storage encryption),   
    IEC 27001/27002 (InfoSec), NERC CIP x, etc., *as appropriate*
6. **Guidance on Newer/Emerging Technologies**  
   Software Defined Network, Cloud Services, Network Virtualization
7. **Appendices** (as needed)

1. Authentication, Authorization, and Auditing [↑](#footnote-ref-1)
2. Zero Touch Deployment [↑](#footnote-ref-2)
3. Fault-management, Configuration, Accounting, Performance, and Security [↑](#footnote-ref-3)