U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – AVIATION & MISSILE CENTER

Guidelines for Implementing a Low Voltage Command Arm Distributed Fuzing System

Mark Etheridge

NDIA Fuze Conference

Buffalo, NY

Approved for Public Release

MISSION

Deliver collaborative and innovative aviation and missile capabilities for responsive and cost-effective research, development and life cycle engineering solutions.

BY THE NUMBERS

~9,553 FY18 Strength

2,943 Civilian

23 Military

6,587 Contractor

FY18 Funding

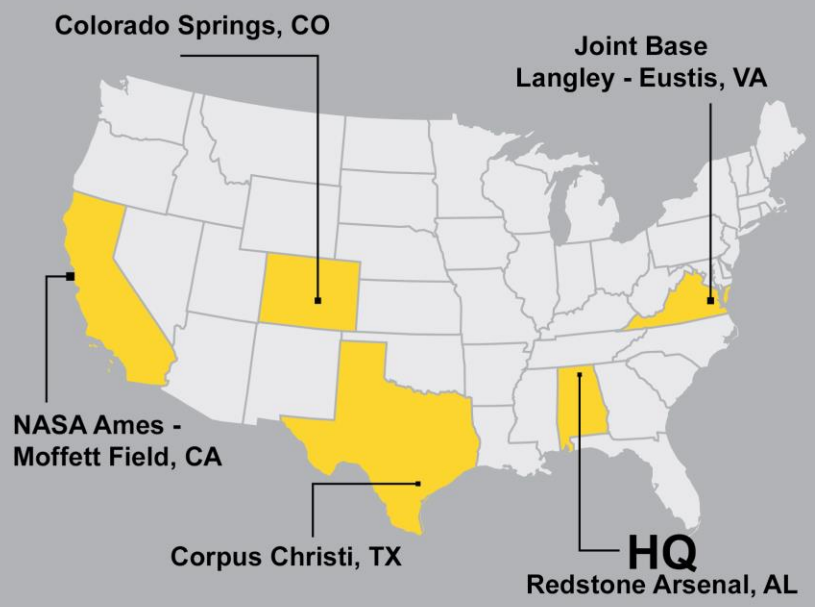
$3.4B

7% Aviation S&T

8% Missile S&T

58% Army

27% Other



Core Competencies

- Life Cycle Engineering
- Research, Technology Development and Demonstration
- Design and Modification
- Software Engineering
- Systems Integration
- Test and Evaluation
- Qualification
- Aerodynamics/ Aeromechanics
- Structures
- Propulsion
- Guidance/Navigation
- Autonomy and Teaming
- Radio Frequency (RF) Technology
- Fire Control Radar Technology
- Image Processing
- Models and Simulation
- Weapons Assurance

PRIORITIES

#1: Readiness

Provide aviation and missile systems solutions to ensure victory on the battlefield today.

#2: Future Force

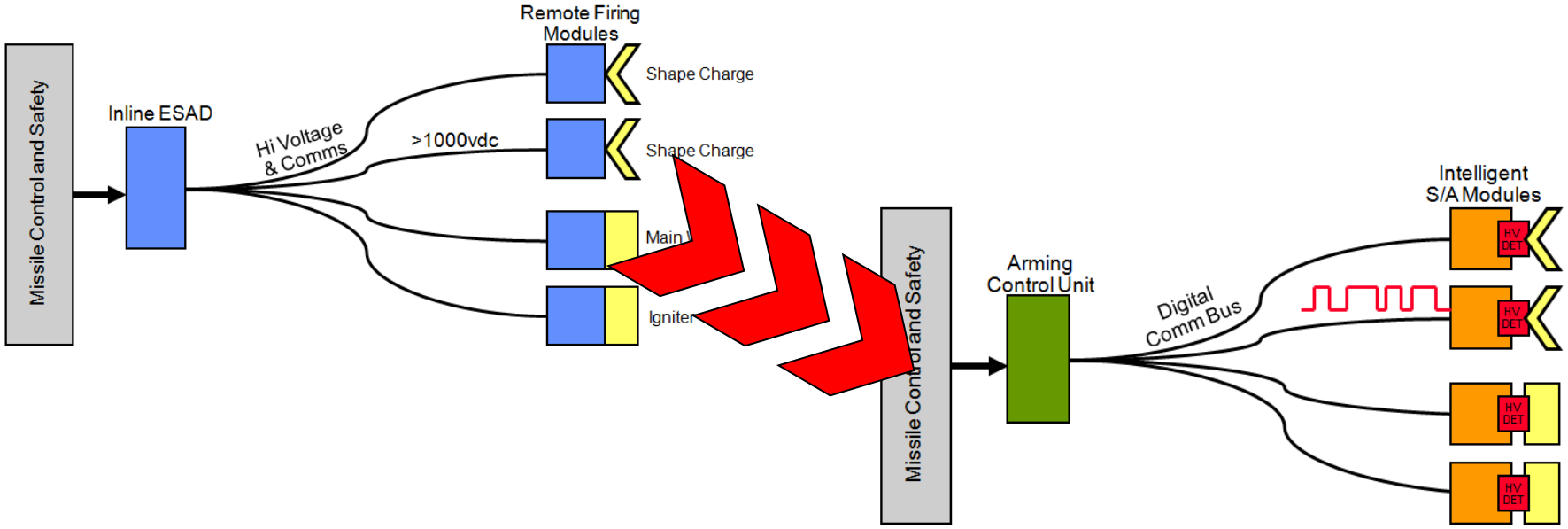
Develop and mature Science and Technology to provide technical capability to our Army's (and nation's) aviation and missile systems.

#3: Soldiers and People

Develop the engineering talent to support both Science and Technology and the aviation and missile materiel enterprise

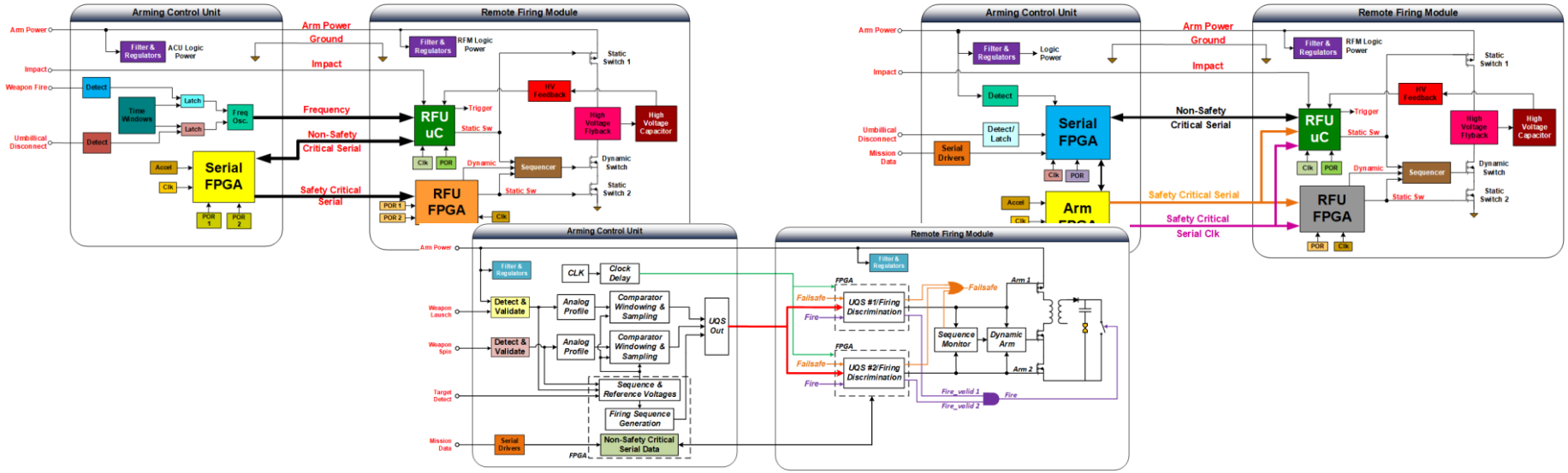
ACKNOWLEDGEMENTS

- **This project is sponsored by the Joint Fuze Technology Panel (JFTP)**
  - FATG II (Tailorable Effects)
- **Alan Durkey, Naval Air Warfare Center**
- **Adedayo Oyelowo, Naval Surface Warfare Center**



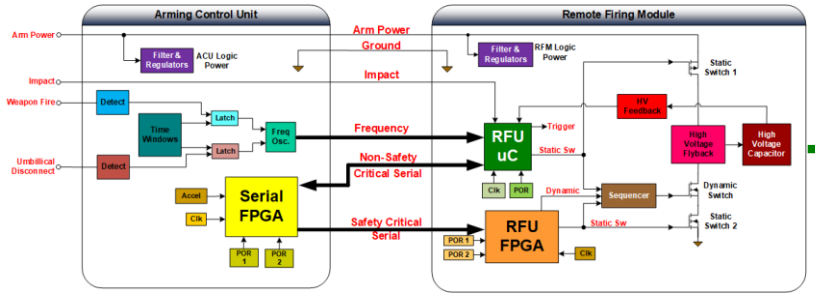
PROJECT HISTORY

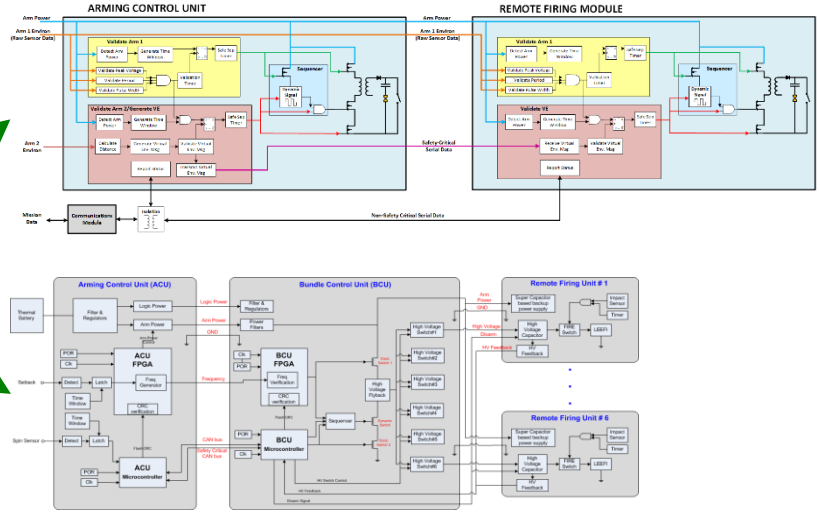
- **This project began in 2010 with a 6.2 effort to develop some generic architectures so as to define some minimal hardware & signal guidelines.**
  - Participants: Army CCDC-AvMC, NAWC, Sandia
  - Architectures: Multiple-Try, Frequency Shift, eUQS
  - Successful in gaining acceptance.
    - FESWG 'approval' in February, 2014
    - FESWG ad-hoc stood up; JOTP document was started.



PROJECT HISTORY

- **A 6.3 program then began in 2015 to pursue form, fit, and function designs with the goal of further defining the 'solution space'**
  - Participants: Army CCDC-AvMC, NAWC, NSWC-IH.
  - Frequency Shift architecture was chosen for implementation
  - Program ending in FY19.
  - Goals met!!
    - Guidelines were refined and new architectures added.





JOTP-054
XXXXXX 2019

DEPARTMENT OF DEFENSE

JOINT ORDNANCE TEST PROCEDURE (JOTP)-054

GUIDELINES FOR THE DESIGN OF LOW VOLTAGE COMMAND-ARM (LVCA) DISTRIBUTED FUZING SYSTEMS

DoD Fuze Engineering Standardization Working Group
(FESWG)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

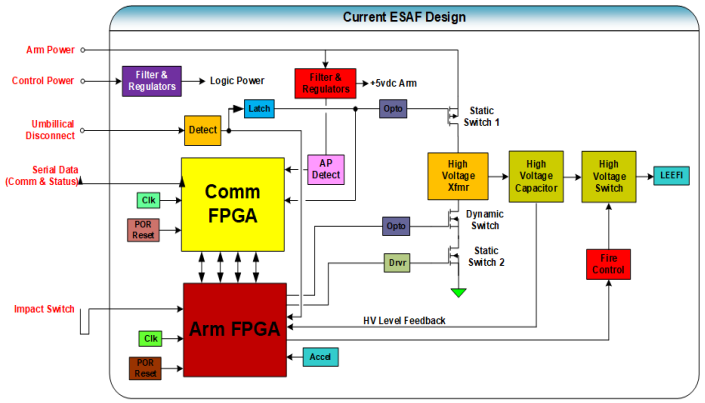
PLEASE NOTE!!

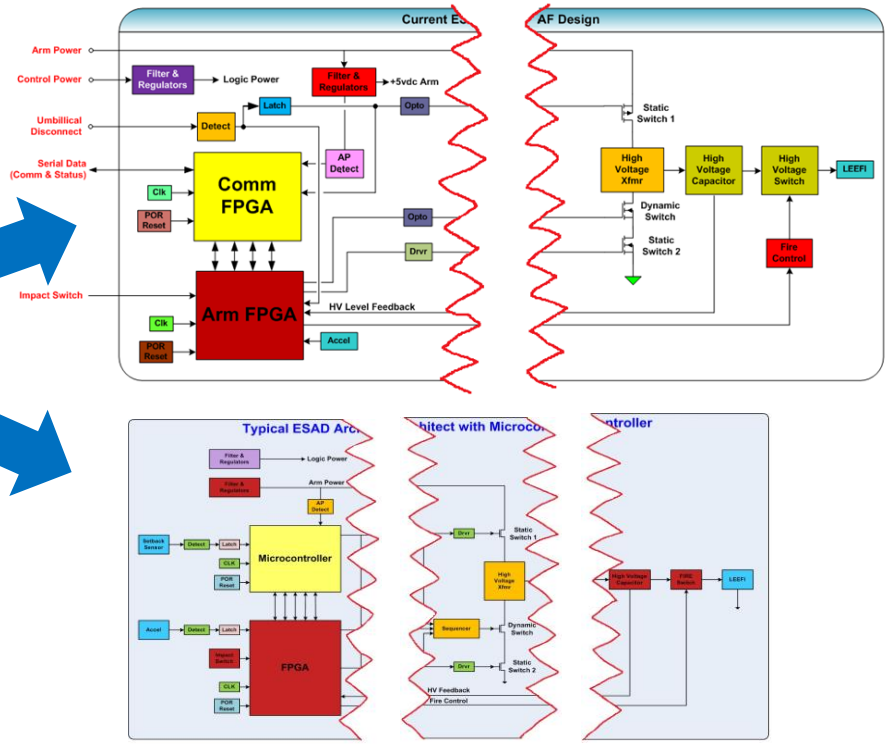
1. **Final review of the document has been completed and the guidelines are being published!!**
2. **The following slides are *guidelines*…not requirements.**
   Consult with the appropriate Service Safety Authority for acceptability if this guidance cannot be adhered too.
3. **Some of the guidelines are not presented.**

DEFINITIONS

Low Voltage Distributed Fuzing/Ignition Architecture

- **A configuration and/or architecture in which elements that influence validation of arming environments are not collocated with the elements that enable safety features..**





DEFINITIONS

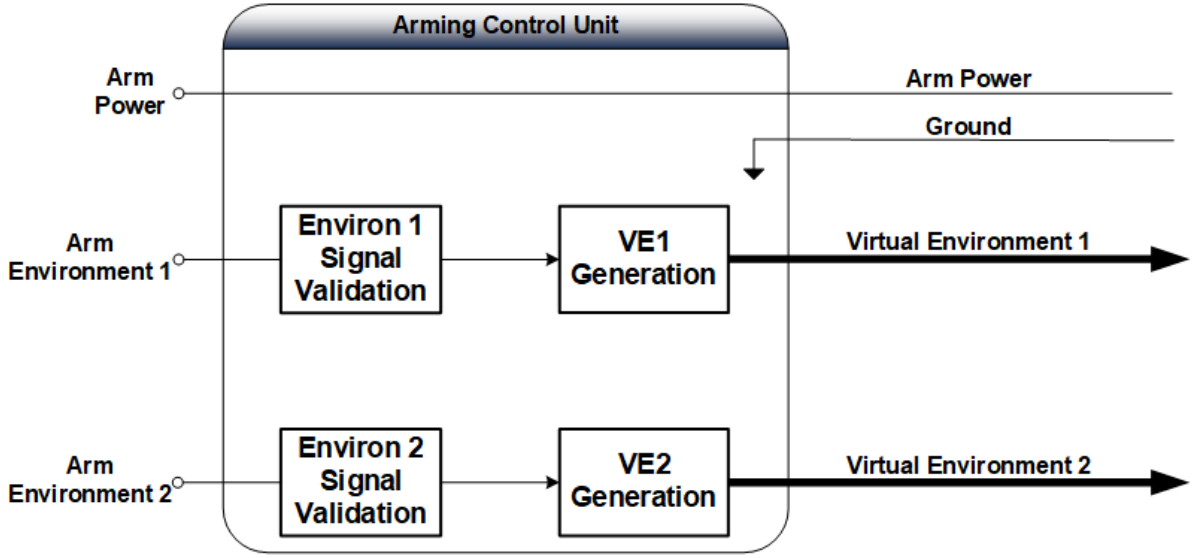
- ***Environment:*** **A specific physical condition to which the fuze and/or ignition system may be exposed.**
- ***Environmental Signal*****: the electrical representation of an environment sensed via transducer or sensor.**
  - Replaced “Arming Signal” in previous presentations
- ***Sensor*****: A component or series of components designed to detect and respond to a specific environment.**
- ***Virtual Environment*****: A unique electrical signal derived or translated from an environmental signal sensed by the fuzing system. It is NOT a direct sensor output.**
  - Encompasses both analog and digital signals
  - VEs are a signal that is designed/engineered to be unique and robust.

Guidelines for the Arming Control Unit

(i.e. the Master S&A)

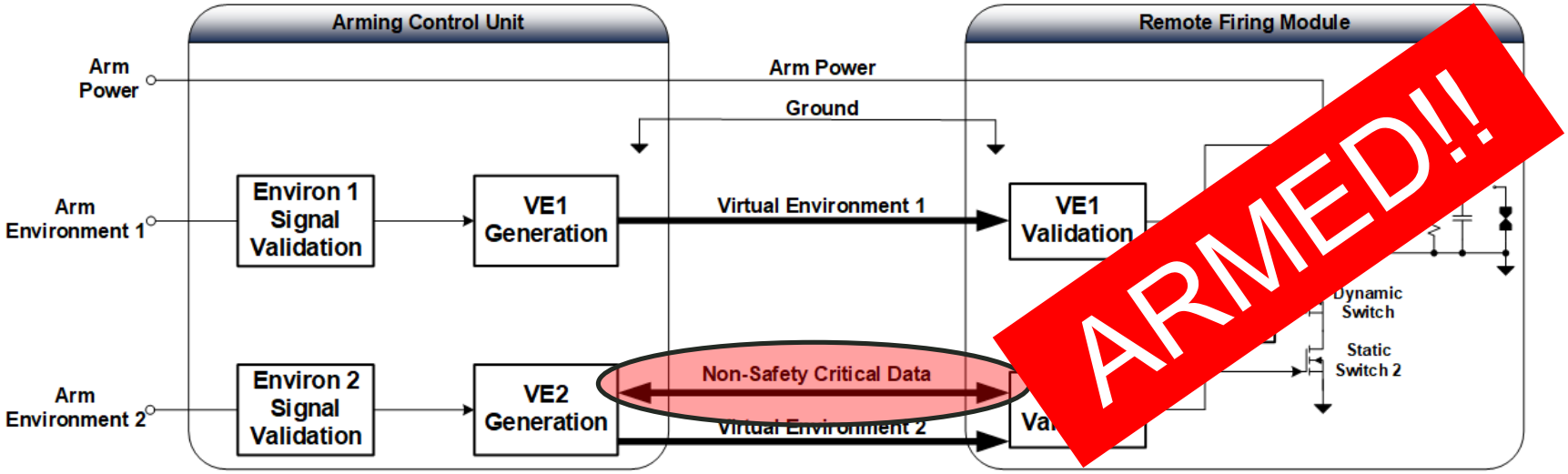
GUIDELINES

- **The Arming Control Unit (ACU) should directly sense, process, and validate at least one physical arming environment. The ACU should translate the physical arming environment(s) into Virtual Environment(s) (VE) and transmit all VE signal(s) to each Remote Firing Module (RFM).**



ACU GUIDELINES

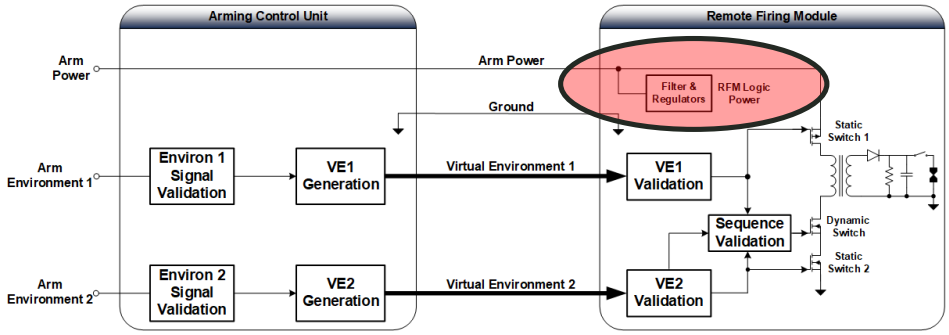
- **Based on system requirements, the ACU may maintain an active link with all RFMs that are in use after the fuze system is properly armed.**



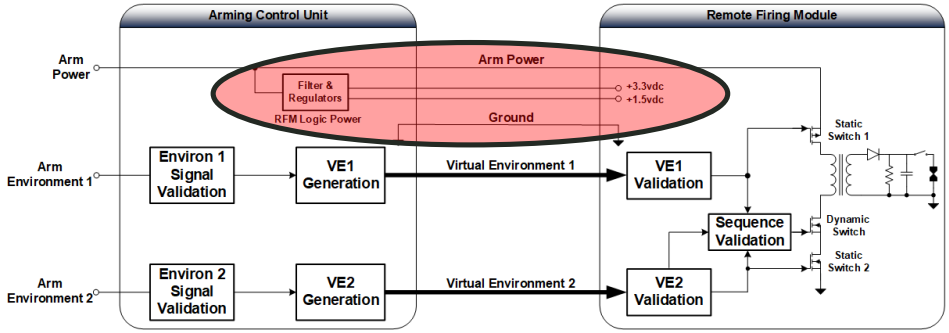
ACU GUIDELINES

- **The ACU is intended to provide all power and ground references for the RFMs including Arm Power where practical.**
  - Can also have the ACU *control* Arm Power to the RFM (ex. Option 3).

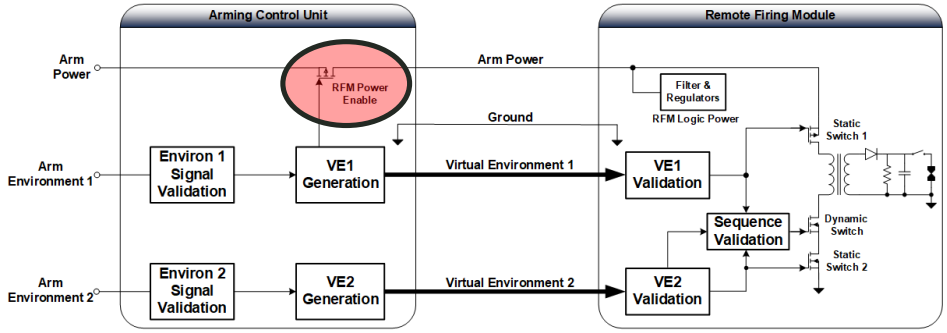
Option 1



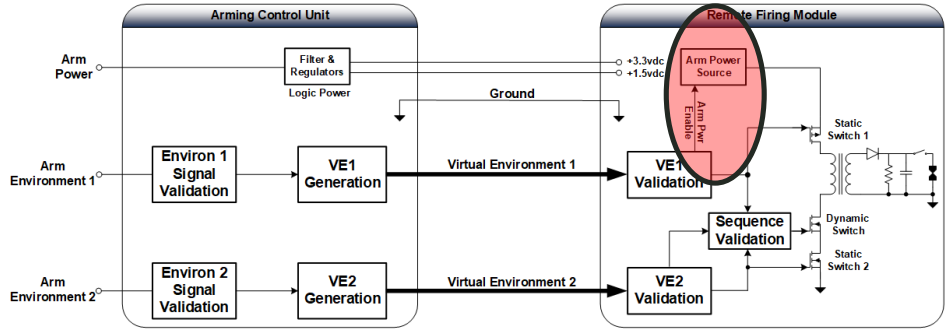
Option 2



Option 3



CONSULT!!!

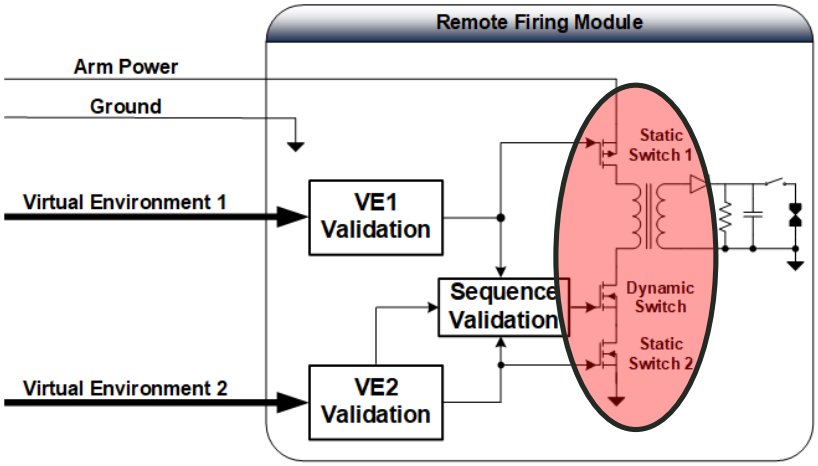


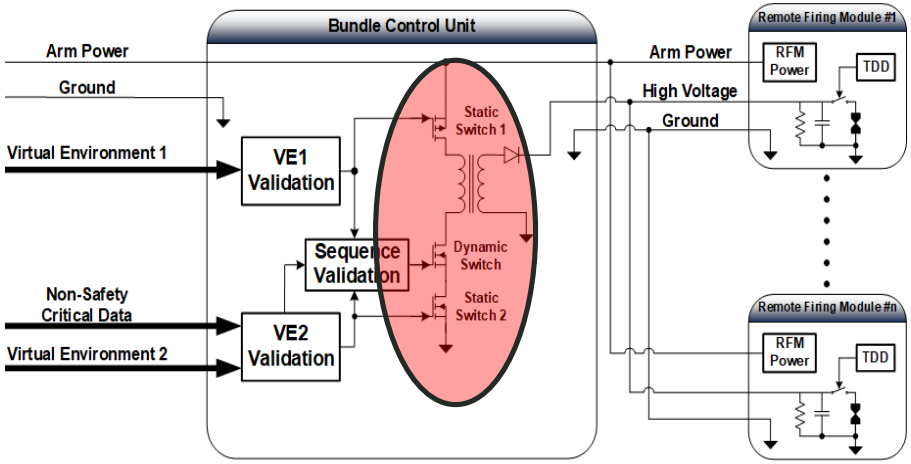
Guidelines for the Remote Firing Module

RFM GUIDELINES

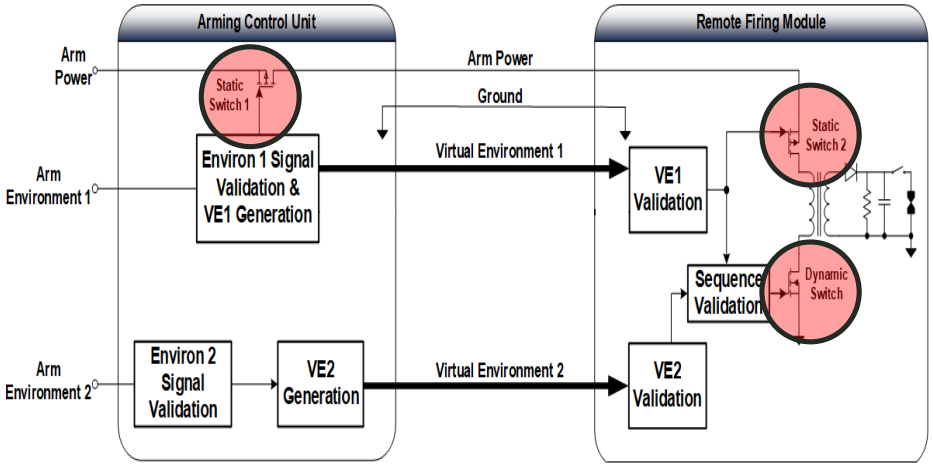
- **The RFM should contain all required arming switches.**

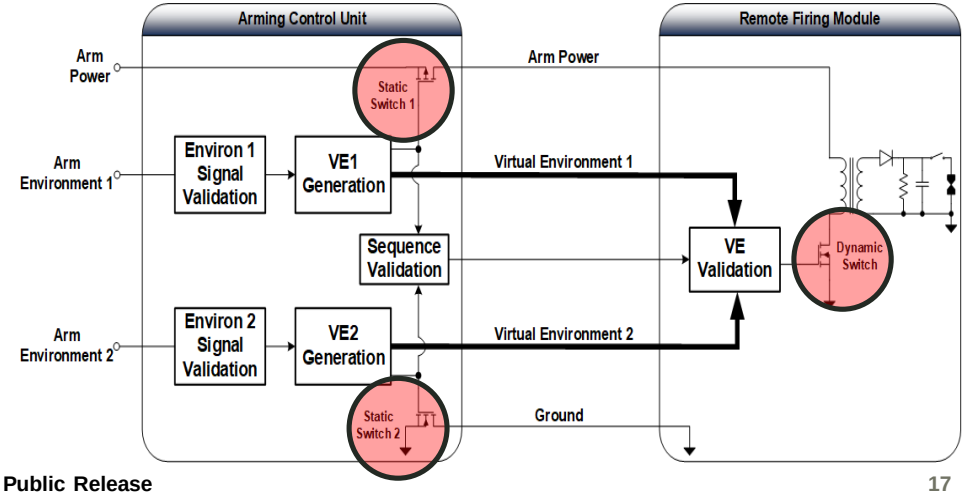
Compliant





CONSULT!!!





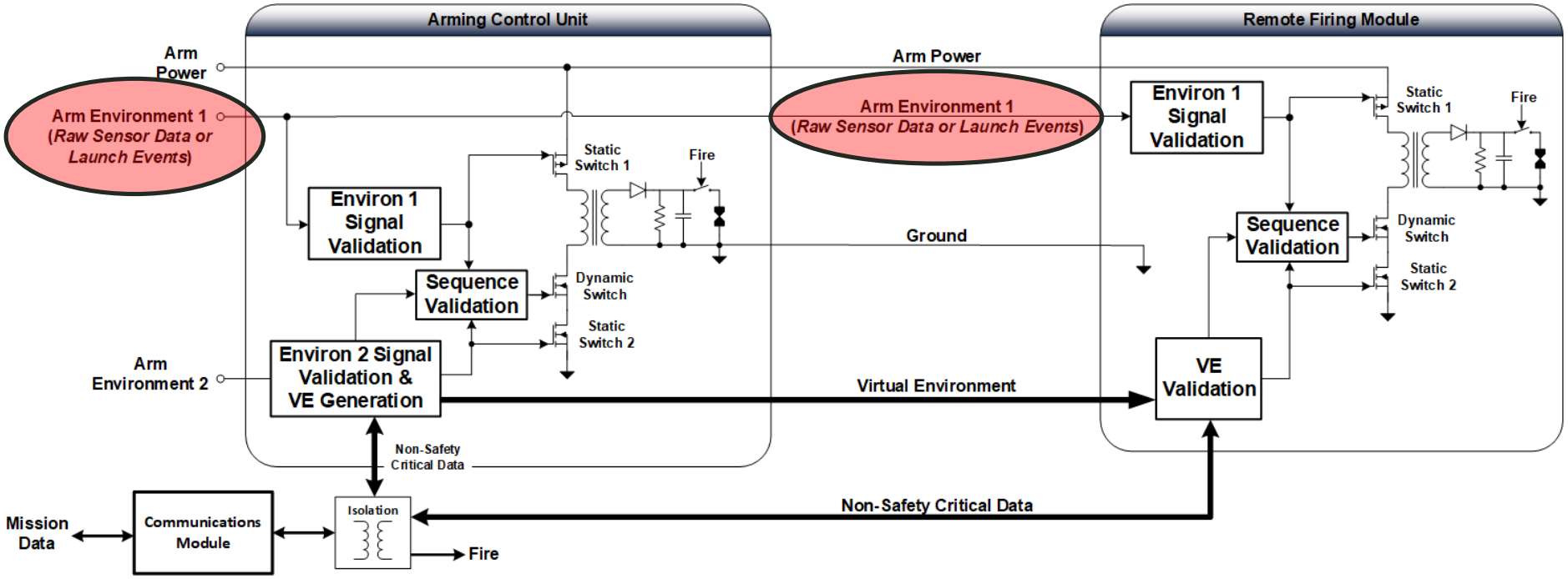
RFM GUIDELINES

- **Power to the safety critical features in the RFM should be applied as late in the launch sequence or operational deployment as practical.**
- **It is preferred that the dynamic signal for driving the high voltage transformer be generated within the RFM.**
- **Timing/Sequencing of the VE signals should be validated within the RFM.**
- **All Arm Delay Timers should reside within the RFM.**

Guidelines for Virtual Environment Signals & Messaging

VIRTUAL ENVIRONMENT GUIDELINES

- **There should be a minimum of two unique VE signals transmitted by the ACU to the RFM for proper arming of the fuze system. *A robust physical environmental signal (i.e., raw sensor data) may be used in lieu of one of the VE arming signals).***

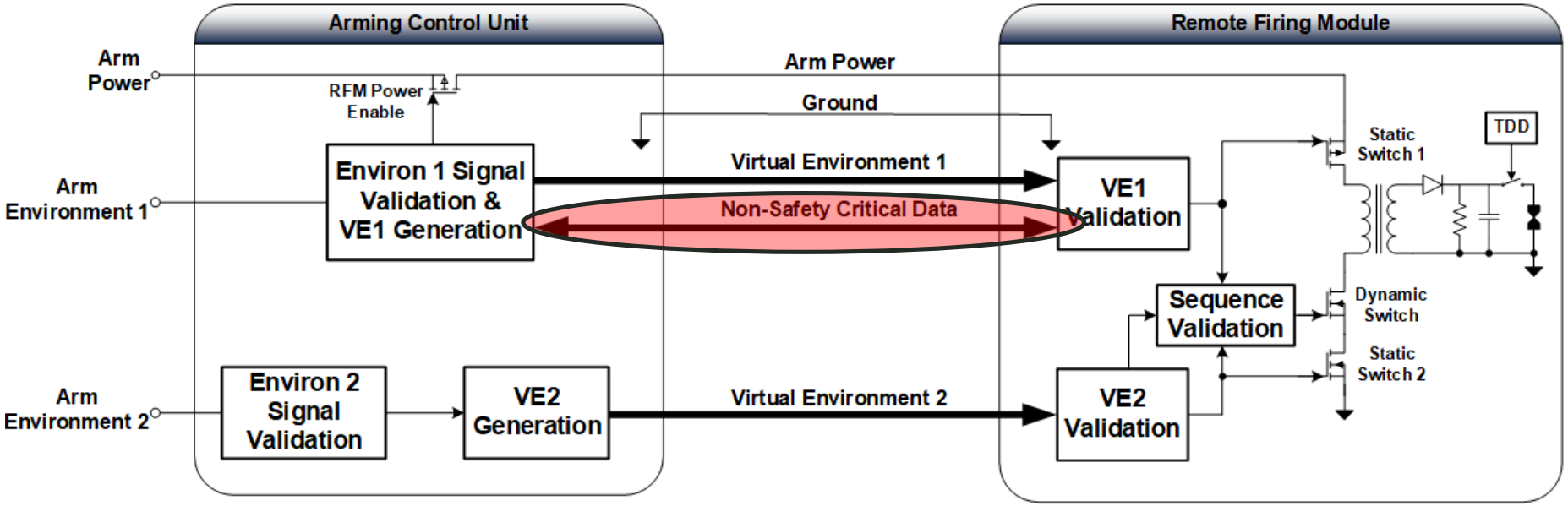


VIRTUAL ENVIRONMENT GUIDELINES

- **All environmental signals and VE signals must be robust such that the signal is not susceptible to inadvertent generation and subversion by credible environments anticipated in the lifecycle.**
- **Each VE signal should be generated by independent and dissimilar logic circuitry that is physically and functionally partitioned. The degree of dissimilarity should be sufficient to ensure that any credible common cause failure mode susceptibility will not result in an inadvertent arming signal transmission in other logic devices and circuits.**
  - This guidance also applies to the processing of the received arming signal at the RFM and subsequent activation of any safety features contained within.

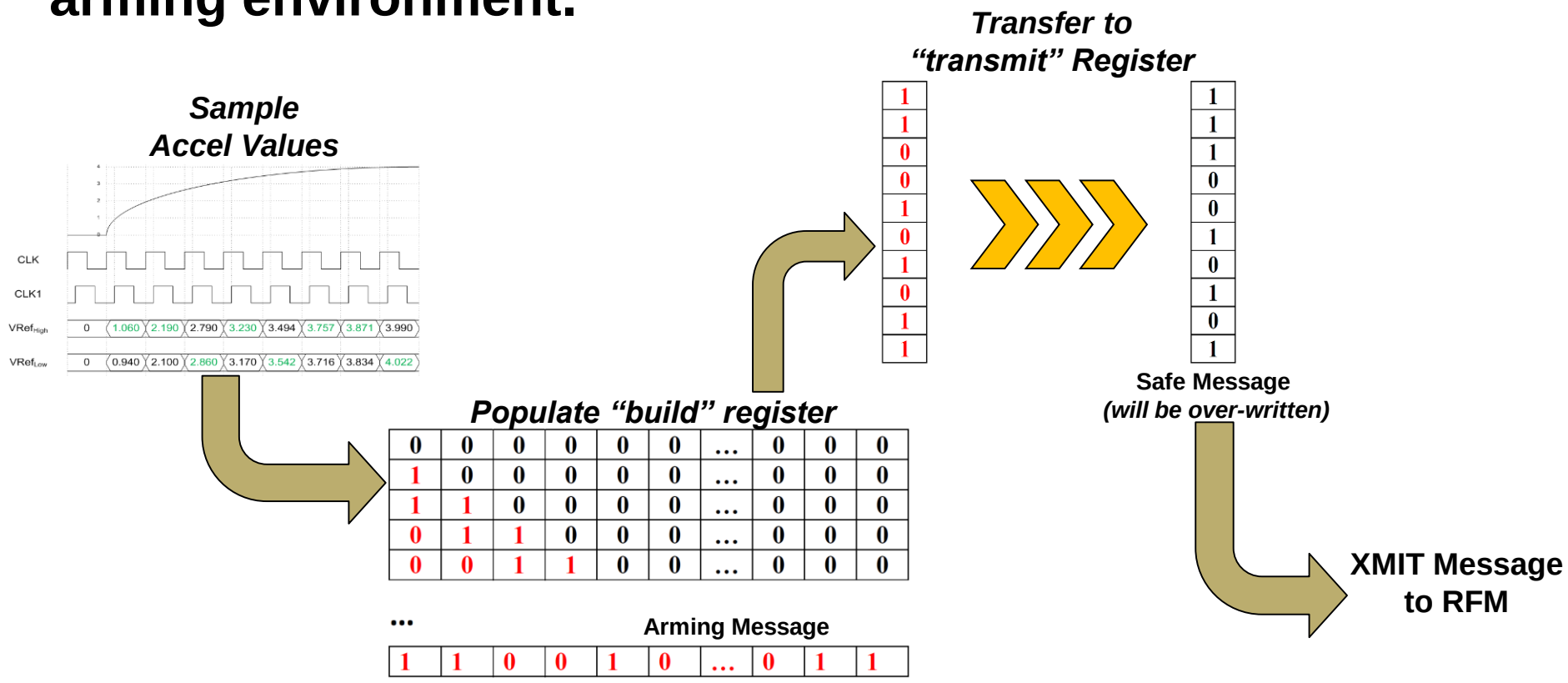
VIRTUAL ENVIRONMENT GUIDELINES

- **Each safety-critical VE message should be implemented as a dedicated, one-way communication line. All non-safety critical messages (e.g., polling, mission data, message acknowledgement, etc.) should be transmitted/received on a separate communication line..**



VIRTUAL ENVIRONMENT GUIDELINES

- **The preferred method is to dynamically generate the VE message based on events that occur throughout an arming environment.**



VIRTUAL ENVIRONMENT GUIDELINES

- **Where generation of the VE message is not practical, pre-stored VE serial messages may be utilized. The pre-stored VE message must be further distinguished by a minimum of two additional validation methods in order to prevent subversion of safety features by credible environments.**
  - Validation methods include but are not limited to…
    - *Sequencing/Sequence Number*
    - *Time Out*
    - *Feedback Message*
    - *Identifiers for sender & receiver*
    - *Alternating messages*
    - *Time Stamp*
    - *Message Reliability (i.e. CRC)*
    - *Flow Control*
    - *Replication*

NOTE: This method is considered a significant risk for acceptable implementation!!! Where operational requirements dictate the use of this method, sufficient justification will need to be provided. Consult with the appropriate SSA.

VIRTUAL ENVIRONMENT GUIDELINES

- **Each VE message should use strong data typing and be unique and unambiguous, from any and all other VE messages.**
  - Error detection schemes (e.g., parity, checksums, CRCs, etc.), if incorporated, must be distinct from any safety-critical message to the extent possible so as to not compromise the integrity of the message.
  - Error correction schemes will not be permitted.

VIRTUAL ENVIRONMENT GUIDELINES

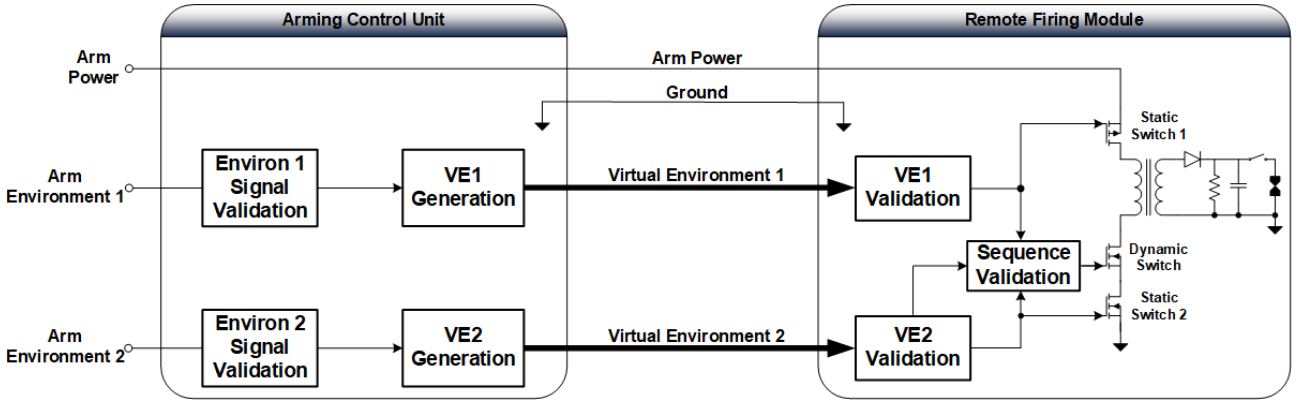
- **Tolerance to corrupt/invalid data should be characterized through analyses and tests. The analyses and test methodologies will be provided to the appropriate SSA for approval.**

Failure Mode	Definition
Inadvertent Release	A class of failures whereby a message is sent that is not a result of deliberate, planned actions
Incorrect Sequence	Messages are not received in the correct order
Early Arrival	The message is received correctly before it is expected
Late Arrival	The message is received correctly later than expected
Repetition	The same message is sent all the time (i.e., babbling idiot)
Deletion	All or part of the messages or message content is missing
Insertion	A message is received unintentionally and is perceived as the correct address (e.g., data from the wrong source)
Corruption	One or more data bits are changed in the message
Masquerade	A non-safety-related message could be interpreted as a safety-related message
Inconsistency	Two or more receivers have a different view of the transmitted data or the receivers may be in different states

Mitigation Method >>>>>>> / Failure Mode	Sequence number	Time Stamp	Time out	Message Reliability (e.g. CRC)	Feedback Message	Flow Control	Identifiers for sender and receiver	Replication	Alternating messages
Inadvertent Release	●	●	●		●				●
Incorrect Sequence	●	●							●
Early Arrival		●							
Late Arrival		●	●		●				
Repetition	●	●							●
Deletion	●	●			●				●
Insertion	●				●			●	●
Corrupted Message				●	●				●
Masquerade				●	●		●		
Inconsistency						●			

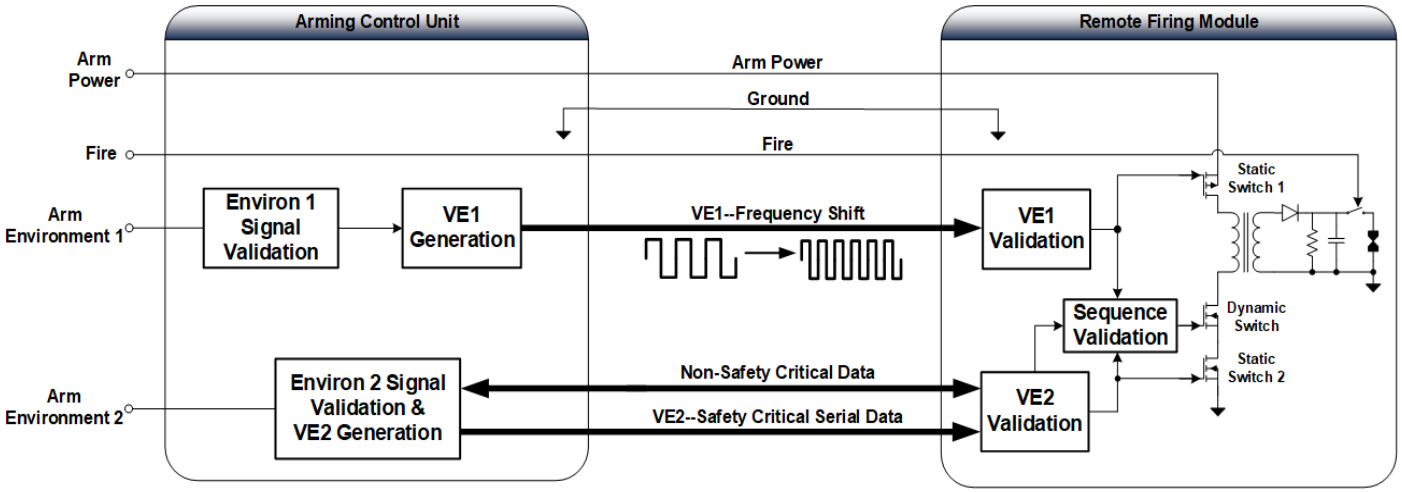
Low Voltage Command-Arm Architectures

FUNDAMENTAL BLOCK DIAGRAM



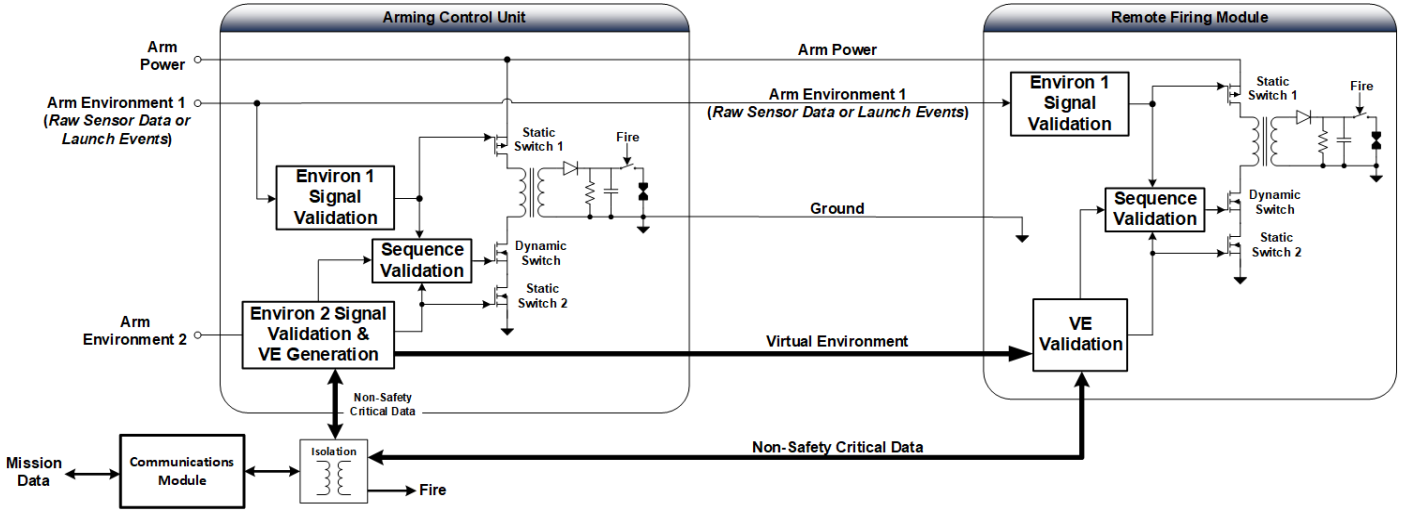
- **The ACU "Environ Signal Validation" & "VE Generation" blocks and the RFM "VE Validation" blocks may be implemented with discrete components or complex logic.**
- **Non-Safety Critical Data (e.g., "Mission" Data) and the "Fire" signals are not shown due to the application-specific nature of these signals.**

FREQUENCY SHIFT/SERIAL DATA BLOCK DIAGRAM



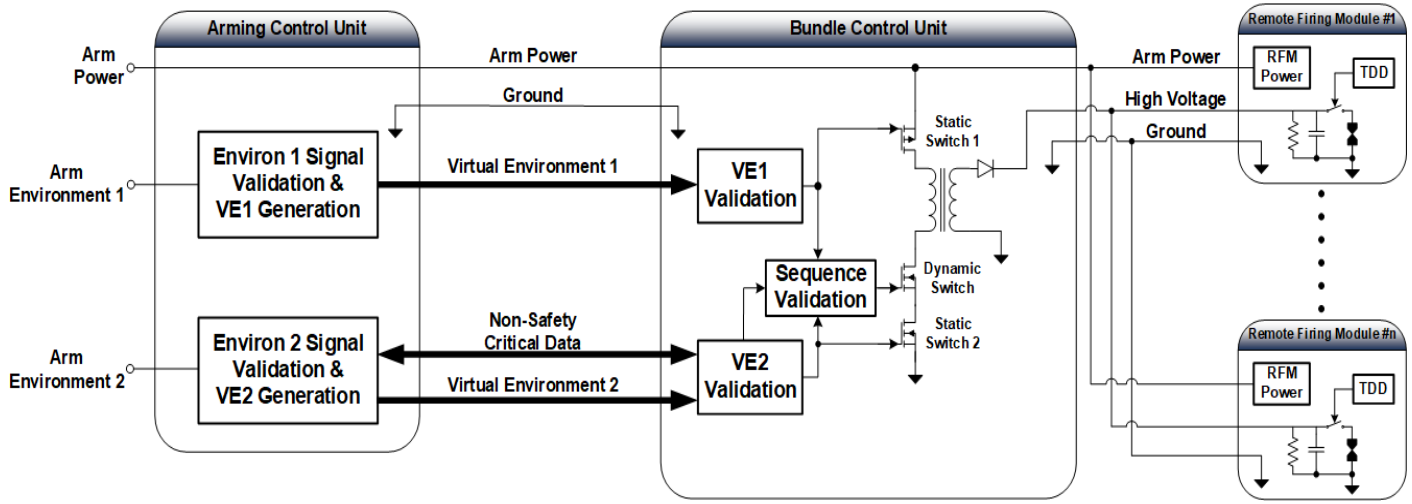
- **An initial frequency is sent to the RFM at the beginning of the arming environment and is "shifted" to another frequency at completion of the arming environment. The RFM must detect this change in frequency within a specific time window for it to be valid.**
- ***Signals Utilized:*** **Analog Square Wave, *Generated* serial message.**

PHYSICAL & VIRTUAL (HYBRID) BLOCK DIAGRAM



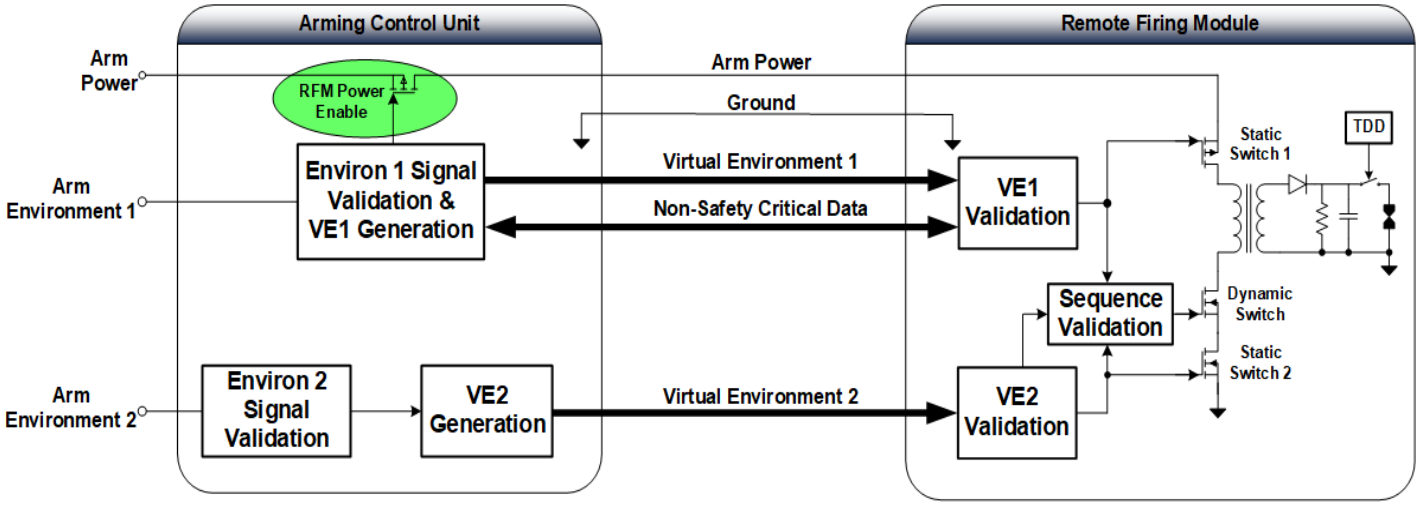
- **This architecture utilizes a robust signal from a physical arming environment and a serial message as a VE. Note that the safety features are located in both the ACU and RFM.**
- ***Signals Utilized:*** **Raw sensor data, *Generated* serial message.**

BUNDLE CONTROL BLOCK DIAGRAM



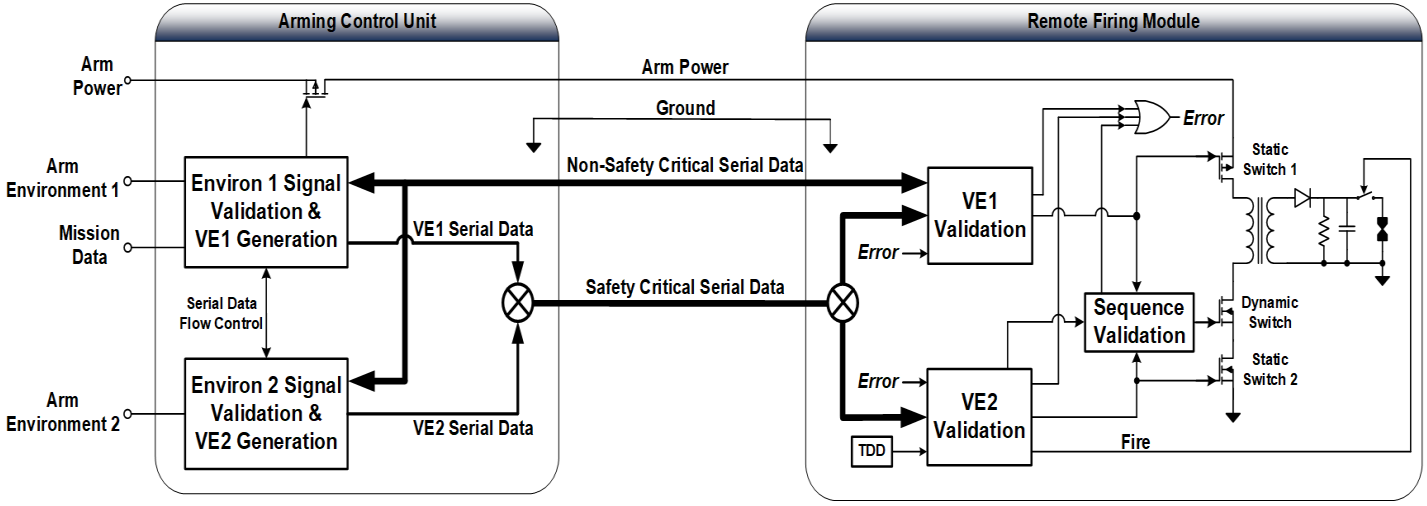
- **This architecture utilizes a centralized safety module and distributes the firing voltage to the remote locations. The VEs are communicated between the ACU and Bundle Control Unit (BCU).**
- ***Signals Utilized:*** **Analog Square Wave (Frequency Shift), *Generated* Controller Area Network (CAN) *broadcast* message.**

RFM POWER CONTROL BLOCK DIAGRAM



- **This architecture utilizes a transistor switch to control power to the RFMs.**
- ***IMPORTANT!!!:*** ***T*****his switch *is not* considered a safety feature and *does not* contribute towards the prevention of fuze arming.**

SINGLE SERIAL DATA LINE BLOCK DIAGRAM



- **In this architecture, both Virtual Environments are transmitted over a single serial data line.**

NOTE: This method is considered a significant risk for acceptable implementation!!! Where operational requirements dictate the use of this method, sufficient justification will need to be provided. Consult with the appropriate SSA.

REFERENCES

- ***Probability of Inadvertent Arming Due to Noise for a Distributed S-A using a Single Serial Data Line*.**
  – Randall Cope, Navy-China Lake; 5 February 1999
- ***Safety of Digital Communications in Machines***
  – Jarmo Alanen et al; VTT Industrial Systems, 2004
- **Validation of Communication in Safety-Critical Control Systems**
  – Jacques Herard et al; Nordtest Technical Report 543; October 2003
- **IEC 61508 – Functional Safety of Electrical Safety-Related Systems**

ALWAYS REMEMBER...WE ARE WITH THE GOVERNMENT AND WE ARE HERE TO HELP!!

QUESTIONS???


You know it's true!!!
I SURVIVED ANOTHER MEETING THAT SHOULD HAVE BEEN AN EMAIL