FF, Dart and Functional Safety
Behind the DART

György Baradits PhD.
SIL4S
 FSM & Competence

- FF
- Functional Safety Management
- DART
History Functional Safety

- First microcomputer based Safety related device
- Oil pipeline Italy-Germany approval distributed electronic protective system
- Y2000 certification
- BP Texas accident
- Dynamic, fail-safe HW systems for large installations
- Bhopal accident
- Piper Alpha accident
- SW quality engineering for large DCS for conventional and nuclear power plants
- Book “Microcomputers in Safety Techniques” published
- National Accreditation Scheme for railroad equipment and information security
- Certification of organizations & People

Accreditation scheme for test and certification bodies in Europe for safety and quality certification of HW and SW of industrial electronics

IEC 61508 Released
IEC 61511 Released
ISA S84 Released

First microcomputer based Safety related device

Plant certification?

Certification of organizations & People
Safety Life Cycle (SLC)

1. Hazard & risk assessment
2. Allocation of safety function to protection layers
3. Safety requirements specification (SRS) for SIS
4. Design and engineering of SIS
5. Installation, commissioning and validation
6. Operation & Maintenance
7. Modification
8. Decommissioning
9. Verification
10. Management of functional safety and functional safety assessment and auditing
11. Safety life-cycle Structure and planning

Analysis
End User/Licensor/Consultant

Realization
Vendor/Contractor/End User

Operation
End User/Contractor

No detailed requirements
Whole life cycle

End User/Licensor/Consultant

Vendor/Contractor/End User
Now normative, previously was informative

Objectives:
- To specify the responsibilities in the management of functional safety
- To specify the activities to be carried out by those with responsibilities in the management of functional safety

Requirements:
- Appointment of one or more persons of an organization with responsibilities
- Identification of all persons responsible for any activities relevant to the achievement of functional safety
- All persons responsible for any activities relevant to the achievement of functional safety shall be competent for the duties they have to perform.
What Is Functional Safety?

- A safety system is functionally safe if
  - *Random*, *common cause* and *systematic* failures do **not** lead to malfunctioning of the safety system and do not result in
    - Injury or death of humans
    - Spills to the environment
    - Loss of equipment or production

**Under its overall life cycle**
Dynamically detecting an ignition

**Ex ib IIC**

**SIL?**

**SRS?**

**Proof test?**

**Validation?**

**Safety System**

**Time to turn-off: 5…10 µs**
Each circuit shall be tested for the following number of revolutions of the wire holder in the spark-test apparatus:

- a) for d.c. circuits - not less than 400 revolutions (5 min.), 200 revolutions at each polarity;

Revolution = on demand
<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Operation: PFD</th>
<th>PFD</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>GE 10^-5 - &lt; 10^-4</td>
<td>10^-4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>GE 10^-4 - &lt; 10^-3</td>
<td>10^-3</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>GE 10^-3 - &lt; 10^-2</td>
<td>10^-2</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>GE 10^-2 - &lt; 10^-1</td>
<td>10^-1</td>
<td>1</td>
</tr>
<tr>
<td>Safety Integrity Level (SIL)</td>
<td>Risk Reduction Factor</td>
<td>Low Demand Mode Operation</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10.000 – 100.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1.000 – 10.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>100 – 1.000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10 – 100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A typical Spark – Electrical Behavior

- Spark Duration
- Initial Phase
- Critical Phase
- $I_s$, $U_s$, $P_s$, $\frac{di}{dt}$
A typical Spark – Extinguished by DART

- Initial Phase
- Critical Phase
- Spark Duration
- \( I_S \)
- \( \frac{dI}{dt} \)
- \( U_S \)
- \( P_S \)
Contributing factors are

- Available power
- System response time
- Energy stored in the connection cable
- Load behavior
DART-Apparatus is certified as intrinsically safe associated apparatus in accordance with IEC60079-11

German metrology institute and notified body PTB has developed the required testing procedures
DART fieldbus provides:

A completely intrinsically safe fieldbus segment for gas groups IIB and IIC with real power redundancy.

Trunk: Full power – Protected by DART,
Spur: All your devices
Main Attributes
- Trunk cable up to 1000 m
- Built-in power redundancy
- Same topology as a general purpose high-power trunk
- For FOUNDATION fieldbus H1 and PROFIBUS PA

DART Fieldbus is certified according to international standard IEC 60079
General Purpose Area

FF Power Supply or PA Segment Coupler

Trunk: increased safety Div. 2 Wiring Method
FieldBarriers
One device per output FISCO or Entity: Ex ia IIC

Zone 1/Class I, Div 2

Terminator

Zone 0/Div. 1
DART: Intrinsically safe High-Power Trunk

General Purpose Area
Zone 2

To DCS
Redundant, three-port isolated
DART Power Supply

The intrinsically safe High-Power Trunk
protected by DART®

DART Segment Protectors

Intrinsically safe spurs
Entity Ex ib IIC

Zone 1
DART: Intrinsically safe High-Power Trunk

- More cable distance
- Higher device count
- Same installation throughout
- Hot work on supplies, couplers, devices

Zone 1
## Technical Data for DART Fieldbus

<table>
<thead>
<tr>
<th>Technical Data</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trunk output power</strong></td>
<td>typ. 22 V / 360 mA</td>
</tr>
<tr>
<td><strong>Spur output power</strong></td>
<td>Min 10.5 @ 34 mA</td>
</tr>
<tr>
<td><strong>Impedance – Cable Type ‘A’</strong></td>
<td>100 Ω</td>
</tr>
<tr>
<td><strong>Trunk cable length, typ. / max.</strong></td>
<td>550 m / 1000 m</td>
</tr>
<tr>
<td><strong>Overall cable length, max. (as per IEC 61158-2)</strong></td>
<td>1900 m</td>
</tr>
<tr>
<td><strong>Spur cable length, max. (as per IEC 61158-2)</strong></td>
<td>120 m</td>
</tr>
</tbody>
</table>

Certified ATEX and IECEx acc. to IEC 60079-11
**Explosion protection compared for fieldbus**

### Output Power P[W]

<table>
<thead>
<tr>
<th>Hazardous Area</th>
<th>FISCO</th>
<th>DART</th>
<th>High-Power Trunk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone 0...1/Div. 1</td>
<td>Zone 1</td>
<td>Zone 0...1/Div. 2</td>
<td></td>
</tr>
<tr>
<td>Gas Group</td>
<td>IIC</td>
<td>IIC</td>
<td>IIC</td>
</tr>
<tr>
<td>Output Values</td>
<td>12.6 V / 100 mA</td>
<td>22.4 V / 360 mA</td>
<td>28 V / 500 mA</td>
</tr>
<tr>
<td>Cable Distance</td>
<td>Medium</td>
<td>Long</td>
<td>Very Long</td>
</tr>
<tr>
<td>Device Count</td>
<td>Low</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>
DART Fieldbus Segment

- DART protects the trunk
  - DART Power Hub:
  - Extinguishes a spark before it becomes incendive
  - Live disconnect permitted without hot work permit
  - Power redundancy with load sharing

- Intrinsically Safe Outputs
  - DART Segment Protector:
  - For any existing standard field instrument
  - Short-circuit protection

=> Intrinsically Safe Ex ib IIC
DART Power Hub

- Redundant Power Supply with load sharing
- With Advanced Diagnostic Module
- DART-protected trunk connection
- Works as I.S. Barrier with three-way galvanic isolation of DCS, bulk power and fieldbus segment

**Technical Data**

<table>
<thead>
<tr>
<th>Trunk Output</th>
<th>DART Power Hub</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rated power</td>
<td>22 V / 360 mA</td>
</tr>
<tr>
<td>DCS supply</td>
<td>10.2 V / 40 mA</td>
</tr>
<tr>
<td>Cable distance, typ./max.</td>
<td>550 m / 1000 m</td>
</tr>
</tbody>
</table>
DART Segment Protector

- Connections for field instrument
- Outputs intrinsically safe Ex ib IIC
- With short-circuit protection
- Live disconnect on trunk and spurs

Technical Data

<table>
<thead>
<tr>
<th>Spur Output</th>
<th>DART Segment Protector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rated power</td>
<td>min 10.5 V @ 34 mA</td>
</tr>
<tr>
<td>IS Power rating</td>
<td>24 V / 250 mA</td>
</tr>
<tr>
<td>Spur length up to</td>
<td>120 m</td>
</tr>
</tbody>
</table>