Safety Design for Operational Effectiveness

Experiences from Use Cases

Presenter: Johann Holm
Organization: North-West University
Contact: johann.holm@nwu.ac.za / 083 453-4314

2007-07-26

Safety and Productivity

- Could also be stated: Safety ***vs*** Productivity;
- Production focus: Safety a secondary requirement
- Safety focus: Production a secondary requirement
- Systems approach: **Integrated** requirements and solution
  - Requirements analysis (operational, legal, etc)
  - Conceptual design (balance requirements and optimize)
  - Preliminary design (identify lower-level optimizations - critical)
  - Detail design and testing (iterative evaluation, optimization)
  - Integration (in-use optimization, ownership)

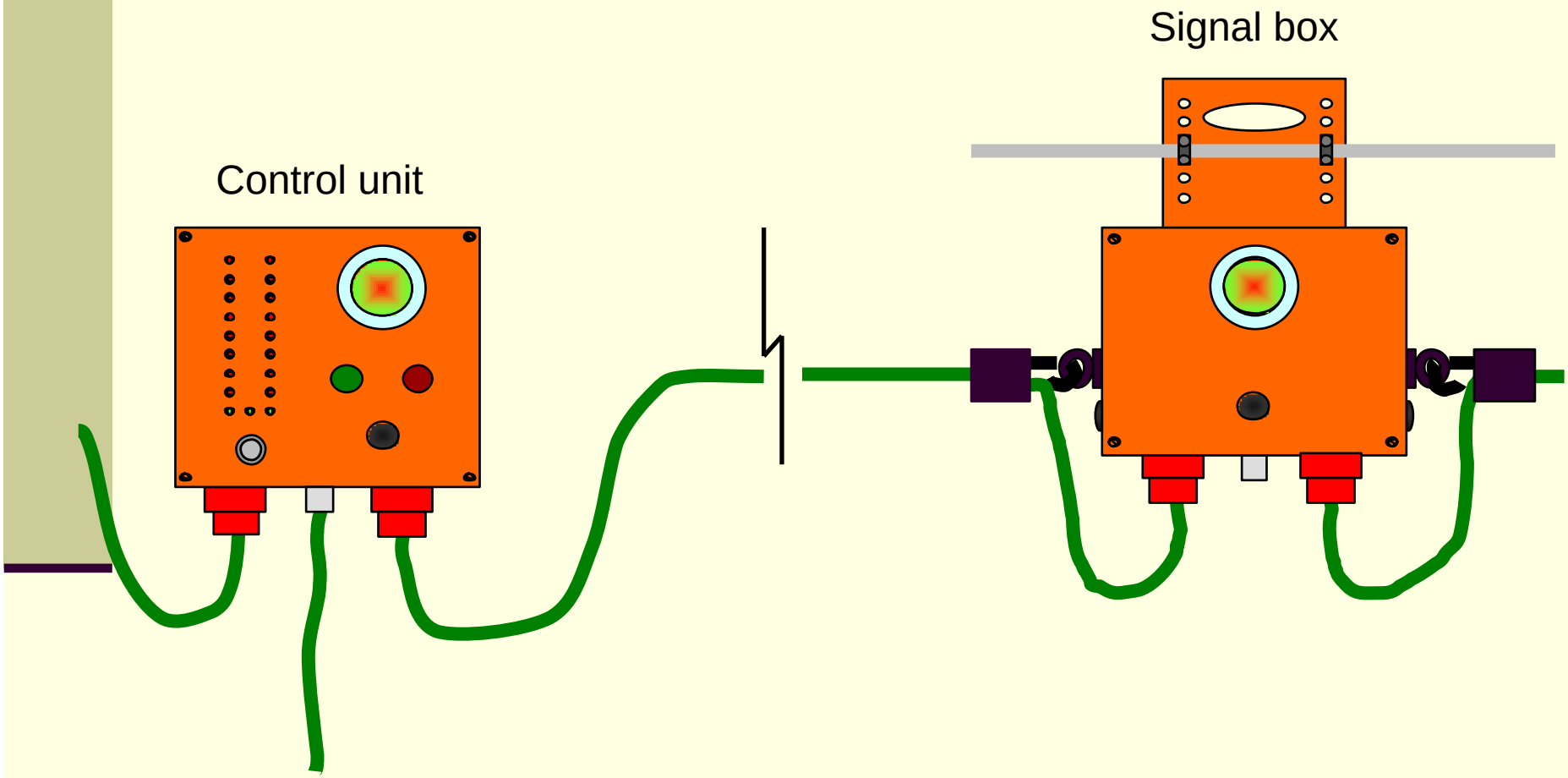
Preliminary Design
(most often neglected)

- Operational architecture
  - Functional units – critical to identify “safe” components
  - Functional interfaces – critical for usability
- Work flow analysis
  - Operational flow
    - Identify critical and “safe” functions – understand users
    - Attempt to preserve people’s habits – integrate solution
  - Technical flow to identify maintenance functions
  - Detail flow to identify critical functions / loops
- Requirements allocation
  - Trace requirements

“Design For” Criteria
(design constraints)

- Functional capability
  - Resource allocation – humans vs equipment
    - Always a trade-off between human and technology
    - Human interface design ensures understanding and safety
    - Human training ensures acceptance and safety
- Performance
- Effectiveness factors
  - Operational availability / reliability
  - **Usability**
  - **Safety**
  - Maintenance, support, environment, etc

Winch Signaling / Safety System (Anglo Platinum)



2007-07-26

Winch Signaling / Safety System (Anglo Platinum)

- Safety and signaling system (concept from mine)
- Followed systems approach
- Developed specification over time (collaborative)
  - Productivity, reliability, safety challenges
- Production functions evolved in specification
  - Did not change operational momentum
  - Tested thoroughly (operational)
  - Implemented and added critical features
  - Well integrated solution that improves safety
  - Solution that effectively increases work flow

Winch Signaling / Safety System (Anglo Platinum)

- FMECA
- Closed-loop state design
- Critical analysis of components
- Simplistic (minimum component) design
- Example:
  - Cable faults
  - Component faults
  - Fail to safe with indication, etc

Winch Signaling System - Video (Anglo Platinum)

- Signal box – installed
- Cable suspension – installed
- Main control unit – installed
- Main control unit - modes of operation
- Slaves and main control unit - signaling

Conclusion

- Safety / operational capability can / must be optimized together
- Do an “as is” analysis first
- Follow a systems engineering approach
- Attempt to maintain existing work flow
- Identify functions and interfaces
- Simplify all user functions and interfaces
- Ensure ownership from personnel

IS Centralized Blasting (Beatrix)

- Initially a safety system (focus)
- Followed a system approach
- Developed specification (collaborative)
- Eventually a production system
  - Involved personnel from onset
  - Listened and performed “as is” analysis
  - Implemented BUT changed procedures
  - Transferred ownership to personnel
  - Always improvements

Ventilation Products

- IS, intelligent power supplies
- IS, easy-to-use methane sensors
- IS, effective ventilation-and-air monitoring
  - Systems approach (installers, users, maintenance)
  - Basic functionality
  - Legal adherence (IS)
  - Calibration / installation support built into equipment
  - Reliability design – fail to safe