



Risk Pilot
Your Risk Navigator



NKS/DIGREL

Basic Concepts

Stefan Authén
Risk Pilot



Digital I&C, what do we mean ?

- A software based digital protection or control system
- Interacts with process systems
- Typical features
 - Includes failure detection and fault-tolerant features.
 - Includes hardware modules such as processors, I/O:s, subracks, process interfaces
 - Software based validation and/or actuation
 - Information exchange by databus within and between divisions



Reliability analysis challenges

- Needs to be quantified in a justifiable manner.
- Needs to evaluate (?)
 - Hardware
 - Software
 - Dynamic interactions
- A number of modeling and data collection challenges exist, and consensus has not yet been reached



Basic Taxonomy

- Main issues a taxonomy needs to consider:
 - Purpose of digital I&C system
 - E.g. RPS or process control
 - Reactor type
 - BWR or PWR
 - Modelling aspects, e.g:
 - Failure detection and actions on detected failure,
 - voting logic,
 - Data bus communication and signal exchanges,
 - spurious activations



Basic Taxonomy, cont.

- Failures and Failure modes , e.g:
 - Hardware, software,
 - Single components / super components
 - Undetected / detected failures,
 - CCF:s

- Hardware Components, e.g:
 - Level of detail
 - Critical equipment

- Failure Data
 - Supplier data / operational experience
 - Independent failures / CCF

- and more.....