Diagnosing Dependent Failures – an Extension of Consistency-based Diagnosis

Jörg Weber and Franz Wotawa

• common assumption in MBD applications: components fail independently
• but: there are cascading faults in some domains (the failure of \( c_i \) causes permanent damage to \( c_j \))
• examples from HW/SW in mobile autonomous robots:
  – SW components are tightly coupled with HW (e.g., camera and image processing software)
  – failures in framework (CORBA,...) may propagate
  – communication does not strictly decouple SW components (e.g., remote procedure calls)
Minimal Diagnosis Environments

Example: robot control system:

- scenario: BD fails, LS and SS try to make RPC to BD and crash
- the minimal diagnosis \{ab(LS), ab(SS)\} does not contain all failed components, repair would fail
- \{ab(BD), ab(LS), ab(SS)\} is insufficient, too: we need to know the failure dependencies for repair
- desired: the MDE \{indf(BD), df(BD, LS), df(BD, SS)\}