Supplementary Material for "System-Theoretic Safety Analysis for Railway Interlocking Systems: From Universal to Station-Specific Requirements"

Appendix A. Unsafe software scenarios

This section provides a detailed presentation of the complete set of Unsafe Software Scenarios (USSs) derived in Section 4.4.

- **USS1**: [Reserve] **Provided** [any] **by the linear segment or turnout controller if** [Mode = ¬Idle]
- **USS2**: [Release] **Provided** [any] **by the linear segment or turnout controller if** [State = Occ]
- **USS3**: [Release] **Provided** [any] **by the linear segment or turnout controller if** [Mode = ResId; Cancel = False]
- **USS4**: [Switch] **Provided** [any] **by the turnout controller if** [Position = Assigned; LockSt = Unlock]
- **USS5**: [Lock] **Provided** [any] **by the turnout controller if** [Position = ¬Assigned; LockSt = Unlock]
- **USS6**: [Unlock] **Provided** [any] **by the turnout controller if** [State=Occ]
- **USS7**: [Unlock] **Provided** [any] **by the turnout controller if** [Mode = ResId; Cancel = False]
- **USS8**: [Reserve] **Provided** [any] **by the route controller if** [Routemode = ¬Marked]
- **USS9**: [Switch] **Provided** [any] **by the route controller if** [Routemode = ¬Reserved]

- **USS10**: [Lock] **Provided** [any] **by the route controller if** [Routemode = ¬Formed]

- **USS11**: [Go] **Provided** [any] **by the route controller if** [Routemode = ¬Available]

- **USS12**: [Cancel] **Provided** [any] **by the route controller if** [Routemode = Occ]

- **USS13**: [Cancel] **Provided** [any] **by the route controller if** [Routemode = Lock; SignalState = Go]

- **USS14**: [Stop] **Provided** [too Late] **by the route controller if** [SignalState = Go; NoMembersOcc = False]

- **USS15**: [Stop] **Not Provided by the route controller if** [SignalState = Go; NoMembersOcc = False]

Appendix B. Universal software safety requirements

This section provides a detailed presentation of the complete set of universal SSRs derived in Section 4.4.

- **Universal SSR1**: [Reserve] **Must Not be Provided** [any] **by the linear segment or turnout controller if** [Mode = ¬Idle]

- **Universal SSR2**: [Release] **Must Not be Provided** [any] **by the linear segment or turnout controller if** [State = Occ]

- **Universal SSR3**: [Release] **Must Not be Provided** [any] **by the linear segment or turnout controller if** [Mode = ResId; Cancel = False]

- **Universal SSR4**: [Switch] **Must Not be Provided** [any] **by the turnout controller if** [Position = Assigned; LockSt = Unlock]

- **Universal SSR5**: [Lock] **Must Not be Provided** [any] **by the turnout controller if** [Position = ¬Assigned; LockSt = Unlock]

- **Universal SSR6**: [Unlock] **Must Not be Provided** [any] **by the turnout controller if** [State=Occ]

- **Universal SSR7**: [Unlock] **Must Not be Provided** [any] **by the turnout controller if** [Mode = ResId; Cancel = False]

- **Universal SSR8**: [Reserve] **Must Not be Provided** [any] **by the route controller if** [Routemode = ¬Marked]

- **Universal SSR9**: [PositionCmd] **Must Not be Provided** [any] **by the route controller if** [Routemode = ¬Reserved]

- **Universal SSR10**: [Lock] **Must Not be Provided** [any] **by the route controller if** [Routemode = ¬Formed]

- **Universal SSR11**: [Go] **Must Not be Provided** [any] **by the route controller if** [Routemode = ¬Available]

- **Universal SSR12**: [Cancel] **Must Not be Provided** [any] **by the route controller if** [Routemode = Occ]

- **Universal SSR13**: [Cancel] **Must Not be Provided** [any] **by the route controller if** [Routemode = Lock; Signalstate=Go]

- **Universal SSR14**: [Stop] **Must be Provided by the route controller if** [SignalState = Go; NoMembersOcc = False]

Appendix C. Specific software safety requirements

This section provides a detailed presentation of the complete set of SSRs specific to Route R3.

- **Specific SSR1-1**: [Reserve] **Must Not be Provided** [any] **by the L11 controller if** [L11Mode = ¬Idle]

- **Specific SSR1-2**: [Reserve] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = ¬Idle]

- **Specific SSR1-3**: [Reserve] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = ¬Idle]

- **Specific SSR2-1**: [Release] **Must Not be Provided** [any] **by the L11 controller if** [L11State = Occ]

- **Specific SSR2-2**: [Release] **Must Not be Provided** [any] **by the T12 controller if** [T12State = Occ]

- **Specific SSR2-3**: [Release] **Must Not be Provided** [any] **by the T13 controller if** [T13State = Occ]

- **Specific SSR3-1**: [Release] **Must Not be Provided** [any] **by the L11 controller if** [L11Mode = ResId; L11Cancel = False]
- **Specific SSR3-2**: [Release] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = ResId; T12Cancel = False]
- **Specific SSR3-3**: [Release] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = ResId; T13Cancel = False]
- **Specific SSR4-1**: [Switch] **Must Not be Provided** [any] **by the T12 controller if** [T12Position = Assigned; T12LockSt = Unlock]
- **Specific SSR4-2**: [Switch] **Must Not be Provided** [any] **by the T13 controller if** [T13Position = Assigned; T13LockSt = Unlock]
- **Specific SSR5-1**: [Lock] **Must Not be Provided** [any] **by the T12 controller if** [T12Position = ¬Assigned; T12LockSt = Unlock]
- **Specific SSR5-2**: [Lock] **Must Not be Provided** [any] **by the T13 controller if** [T13Position = ¬Assigned; T13LockSt = Unlock]
- **Specific SSR6-1**: [Unlock] **Must Not be Provided** [any] **by the T12 controller if** [T12State = Occ]
- **Specific SSR6-2**: [Unlock] **Must Not be Provided** [any] **by the T13 controller if** [T13State = Occ]
- **Specific SSR7-1**: [Unlock] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = ResId; T12Cancel = False]
- **Specific SSR7-2**: [Unlock] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = ResId; T13Cancel = False]
- **Specific SSR8-1**: [Reserve] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Marked]
- **Specific SSR9-1**: [PositionCmd] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Reserved]
- **Specific SSR9-2**: [PositionCmd] **Must Not be Provided** [any] **by the R3 controller if** [L11Mode = ¬ResId || T12Mode = ¬ResId || T13Mode = ¬ResId]
- **Specific SSR10-1**: [Lock] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Formed]

- **Specific SSR10-2**: [Lock] **Must Not be Provided** [any] **by the R3 controller if** [T12Position = Minus || T13Position = Minus]
- **Specific SSR11-1**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Available]
- **Specific SSR11-2**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [T12LockSt = Unlock || T13LockSt = Unlock]
- **Specific SSR12-1**: [Cancel] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = Occ]
- **Specific SSR13-1**: [Cancel] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = Lock; SG3state=Go]
- **Specific SSR14-1**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; L11State = Occ]
- **Specific SSR14-2**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; T12State = Occ]
- **Specific SSR14-3**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; T13State = Occ]