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

Appendix A. Unsafe Control Actions

This section provides a detailed presentation of the complete set of Unsafe Control Actions (UCAs) derived in Section 4.3.

- **UCA1**: [Reserve] **Provided by the linear segment controller** [any] **is hazardous when** [Mode = ¬Idle; ResId = ¬Null].
- **UCA2**: [Release] **Provided by the linear segment controller** [any] **is hazardous when** [State = Occ].
- **UCA3**: [Release] **Provided by the linear segment controller** [any] **is hazardous when** [Mode = Res; Cancel = False].
- **UCA4**: [Reserve] **Provided by the turnout controller** [any] **is hazardous when** [Mode = ¬Idle; ResId = ¬Null].
- **UCA5**: [Release] **Provided by the turnout controller** [any] **is hazardous when** [State = Occ].
- **UCA6**: [Release] **Provided by the turnout controller** [any] **is hazardous when** [Mode = Res; Cancel = False].
- **UCA7**: [Unlock] **Provided by the turnout controller** [any] **is hazardous when** [State = Occ].
- **UCA8**: [Unlock] **Provided by the turnout controller** [any] **is hazardous when** [Mode = Res; Cancel = False].
- **UCA9**: [Reserve] **Provided by the route controller** [any] **is hazardous when** [RouteMode = ¬Marked; MembersMode = ¬Idle].

- **UCA10**: [Go] **Provided by the route controller** [any] **is hazardous when** [MembersMode = ¬Res].
- **UCA11**: [Go] **Provided by the route controller** [any] **is hazardous when** [TurnoutsLocked = False].
- **UCA12**: [Go] **Provided by the route controller** [any] **is hazardous when** [TurnoutsAligned = False].
- **UCA13**: [Go] **Provided by the route controller** [any] **is hazardous when** [NoMembersOcc = False].
- **UCA14**: [Cancel] **Provided by the route controller** [any] **is hazardous when** [RouteMode = Occ].
- **UCA15**: [Cancel] **Provided by the route controller** [any] **is hazardous when** [RouteMode = Locked; SignalState = Go].
- **UCA16**: [Stop] **Provided by the route controller** [too late] **is hazardous when** [SignalState = Go; NoMembersOcc = False].
- **UCA17**: [Stop] **Not Provided by the route controller is hazardous when** [SignalState = Go; NoMembersOcc = False].

Appendix B. 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 controller if** [Mode = ¬Idle; ResId = ¬Null].
- **USS2**: [Release] **Provided** [any] **by the linear segment controller if** [State = Occ].
- **USS3**: [Release] **Provided** [any] **by the linear segment controller if** [Mode = Res; Cancel = False].
- **USS4**: [Reserve] **Provided** [any] **by the turnout controller if** [Mode = ¬Idle; ResId = ¬Null].
- **USS5**: [Release] **Provided** [any] **by the turnout controller if** [State = Occ].

- **USS6**: [Release] **Provided** [any] **by the turnout controller if** [Mode = Res; Cancel = False].
- **USS7**: [Unlock] **Provided** [any] **by the turnout controller if** [State=Occ].
- **USS8**: [Unlock] **Provided** [any] **by the turnout controller if** [Mode = Res; Cancel = False].
- **USS9**: [Reserve] **Provided** [any] **by the route controller if** [RouteMode = ¬Marked; MembersMode = ¬Idle].
- **USS10**: [Go] **Provided** [any] **by the route controller if** [MembersMode = ¬Res].
- **USS11**: [Go] **Provided** [any] **by the route controller if** [TurnoutsLocked = False].
- **USS12**: [Go] **Provided** [any] **by the route controller if** [TurnoutsAligned = False].
- **USS13**: [Go] **Provided** [any] **by the route controller if** [NoMembersOcc = False].
- **USS14**: [Cancel] **Provided** [any] **by the route controller if** [RouteMode = Occ].
- **USS15**: [Cancel] **Provided** [any] **by the route controller if** [RouteMode = Locked; SignalState = Go].
- **USS16**: [Stop] **Provided** [too Late] **by the route controller if** [SignalState = Go; NoMembersOcc = False].
- **USS17**: [Stop] **Not Provided by the route controller if** [SignalState = Go; NoMembersOcc = False].

Appendix C. 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 controller if** [Mode = ¬Idle; ResId = ¬Null].

- **Universal SSR2**: [Release] **Must Not be Provided** [any] **by the linear segment controller if** [State = Occ].
- **Universal SSR3**: [Release] **Must Not be Provided** [any] **by the linear segment controller if** [Mode = Res; Cancel = False].
- **Universal SSR4**: [Reserve] **Must Not be Provided** [any] **by the turnout controller if** [Mode = ¬Idle; ResId = ¬Null].
- **Universal SSR5**: [Release] **Must Not be Provided** [any] **by the turnout controller if** [State = Occ].
- **Universal SSR6**: [Release] **Must Not be Provided** [any] **by the turnout controller if** [Mode = Res; Cancel = False].
- **Universal SSR7**: [Unlock] **Must Not be Provided** [any] **by the turnout controller if** [State = Occ].
- **Universal SSR8**: [Unlock] **Must Not be Provided** [any] **by the turnout controller if** [Mode = Res; Cancel = False].
- **Universal SSR9**: [Reserve] **Must Not be Provided** [any] **by the route controller if** [RouteMode = ¬Marked; MembersMode = ¬Idle].
- **Universal SSR10**: [Go] **Must Not be Provided** [any] **by the route controller if** [MembersMode = ¬Res].
- **Universal SSR11**: [Go] **Must Not be Provided** [any] **by the route controller if** [TurnoutsLocked = False].
- **Universal SSR12**: [Go] **Must Not be Provided** [any] **by the route controller if** [TurnoutsAligned = False].
- **Universal SSR13**: [Go] **Must Not be Provided** [any] **by the route controller if** [NoMembersOcc = False].
- **Universal SSR14**: [Cancel] **Must Not be Provided** [any] **by the route controller if** [RouteMode = Occ].
- **Universal SSR15**: [Cancel] **Must Not be Provided** [any] **by the route controller if** [RouteMode = Locked; Signalstate = Go].
- **Universal SSR16**: [Stop] **Must be Provided immediately by the route controller if** [SignalState = Go; NoMembersOcc = False].
- **Universal SSR17**: [Stop] **Must be Provided by the route controller if** [SignalState = Go; NoMembersOcc = False].

Appendix D. 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; L11ResId = ¬Null]
- **Specific SSR2-1**: [Release] **Must Not be Provided** [any] **by the L11 controller if** [L11State = Occ]
- **Specific SSR3-1**: [Release] **Must Not be Provided** [any] **by the L11 controller if** [L11Mode = Res; L11Cancel = False]
- **Specific SSR4-1**: [Reserve] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = ¬Idle; T12ResId = ¬Null]
- **Specific SSR4-2**: [Reserve] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = ¬Idle; T12ResId = ¬Null]
- **Specific SSR5-1**: [Release] **Must Not be Provided** [any] **by the T12 controller if** [T12State = Occ]
- **Specific SSR5-2**: [Release] **Must Not be Provided** [any] **by the T13 controller if** [T13State = Occ]
- **Specific SSR6-1**: [Release] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = Res; T12Cancel = False]
- **Specific SSR6-2**: [Release] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = Res; T13Cancel = False]
- **Specific SSR7-1**: [Unlock] **Must Not be Provided** [any] **by the T12 controller if** [T12State = Occ]
- **Specific SSR7-2**: [Unlock] **Must Not be Provided** [any] **by the T13 controller if** [T13State = Occ]
- **Specific SSR8-1**: [Unlock] **Must Not be Provided** [any] **by the T12 controller if** [T12Mode = Res; T12Cancel = False]
- **Specific SSR8-2**: [Unlock] **Must Not be Provided** [any] **by the T13 controller if** [T13Mode = Res; T13Cancel = False]

- **Specific SSR9-1**: [Reserve] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Marked; L11Mode = ¬Idle]
- **Specific SSR9-2**: [Reserve] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Marked; T12Mode = ¬Idle]
- **Specific SSR9-3**: [Reserve] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = ¬Marked; T13Mode = ¬Idle]
- **Specific SSR10-1**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [L11Mode = ¬Res || T12Mode = ¬Res ||T13Mode = ¬Res]
- **Specific SSR11-1**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [T12LockSt = Unlock || T13LockSt = Unlock]
- **Specific SSR12-1**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [T12Position = Minus || T13Position = Minus]
- **Specific SSR13-1**: [Go] **Must Not be Provided** [any] **by the R3 controller if** [L11State = Occ || T12State = Occ || T13State = Occ]
- **Specific SSR14-1**: [Cancel] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = Occ]
- **Specific SSR15-1**: [Cancel] **Must Not be Provided** [any] **by the R3 controller if** [R3mode = Locked; SG3state = Go]
- **Specific SSR16-1**: [Stop] **Must be Provided immediately by the route controller if** [SignalState = Go; L11State = Occ].
- **Specific SSR16-2**: [Stop] **Must be Provided immediately by the route controller if** [SignalState = Go; T12State = Occ].
- **Specific SSR16-3**: [Stop] **Must be Provided immediately by the route controller if** [SignalState = Go; T13State = Occ].
- **Specific SSR17-1**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; L11State = Occ]
- **Specific SSR17-2**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; T12State = Occ]
- **Specific SSR17-3**: [Stop] **Must be Provided by the R3 controller if** [SG3State = Go; T13State = Occ]