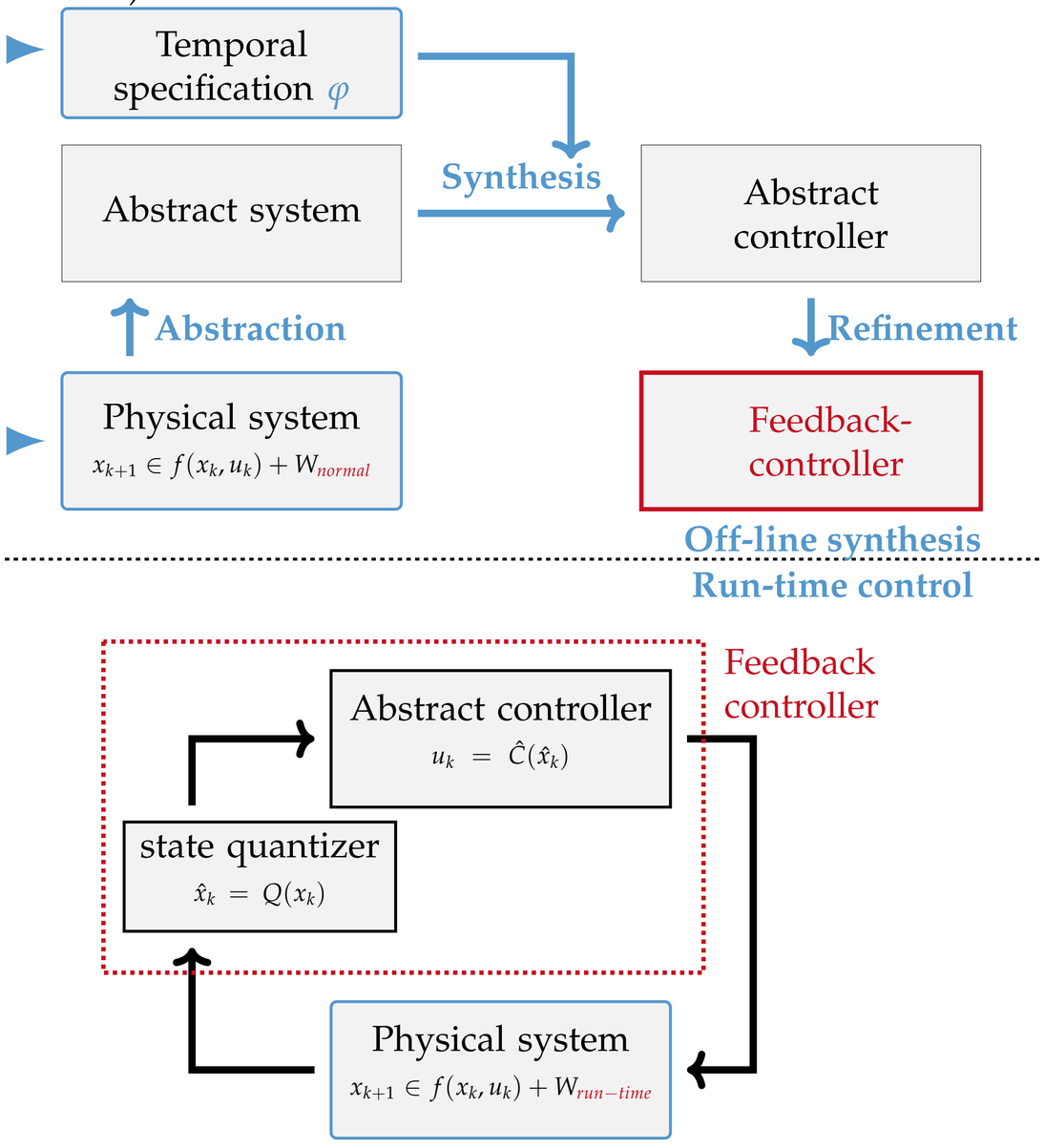
Resilient Abstraction-Based Controller Design

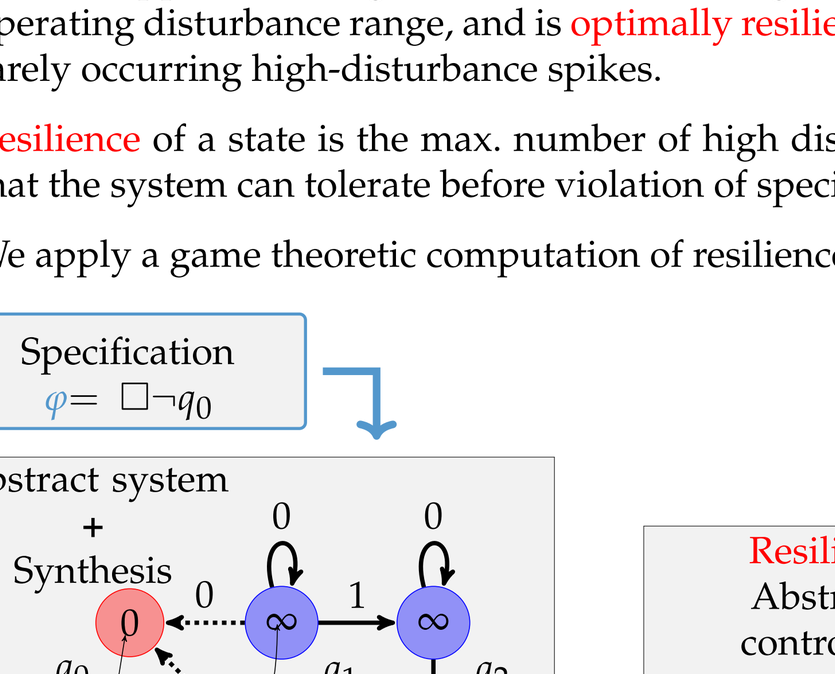
Stanly Samuel[+], Kaushik Mallik[*], Anne-Kathrin Schmuck[*], and Daniel Neider[*]

[+]Indian Institute of Science (IISc), India.
[*]Max Planck Institute for Software Systems (MPI-SWS), Germany.

Abstraction-Based Controller Design (ABCD)

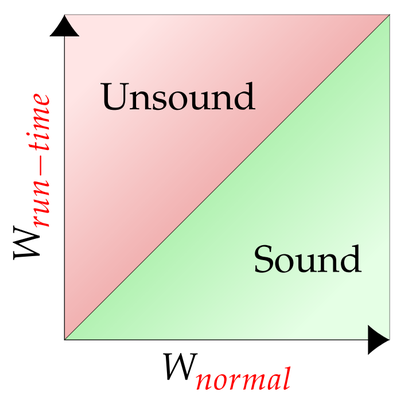
- **System**: Continuous non-linear dynamics
- **Specification**: Discrete, temporal properties (e.g. given in LTL)

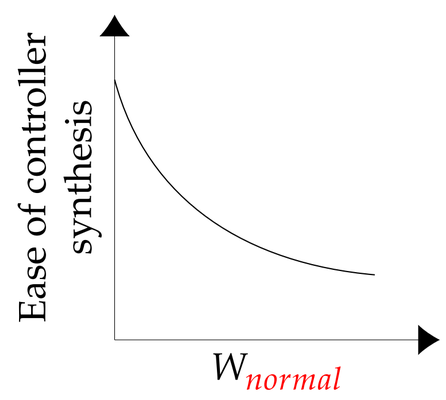




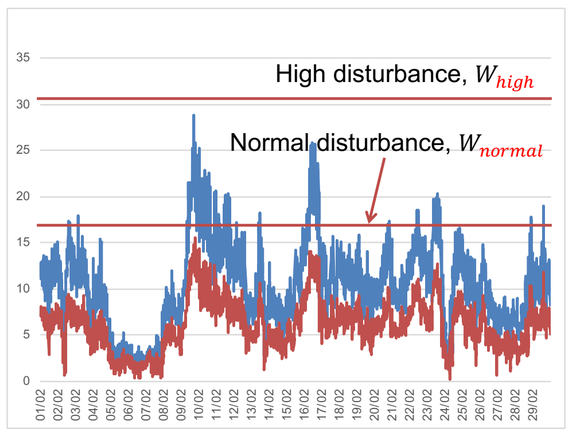
Limitation of a uniform disturbance bound in ABCD

- A synthesized controller is sound if $W_{normal} \geq W_{run-time}$.
- For higher W_{normal}, finding a controller becomes difficult.





- In practice, we encounter milder disturbances most of the time, and more severe disturbances only occasionally. So it is impractical to assume the worst situation all the time.
- Recorded maximum (blue) and average (red) wind speed in m/s in Aachen-Hörn, Germany throughout February 2020:



Data taken from https://www.klimageo.rwth-aachen.de/

Our contribution: Resilient ABCD

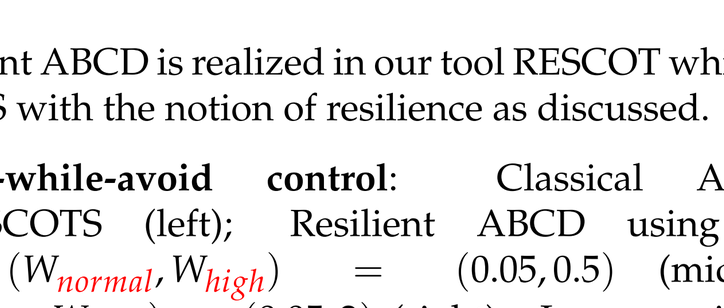
- A novel approach that guarantees soundness against normal operating disturbance range, and is optimally resilient against rarely occurring high-disturbance spikes.
- Resilience of a state is the max. number of high disturbances that the system can tolerate before violation of specification.
- We apply a game theoretic computation of resilience [1].

[1] Neider, D. et al., *Synthesizing optimally resilient controllers*, Acta Informatica, 2020.

Experimental evaluation

- Resilient ABCD is realized in our tool RESCOT which extends SCOTS with the notion of resilience as discussed.
- **Reach-while-avoid control**: Classical ABCD using SCOTS (left); Resilient ABCD using RESCOT with $(W_{normal}, W_{high}) = (0.05, 0.5)$ (middle) and $(W_{normal}, W_{high}) = (0.05, 2)$ (right). Lower resilient states are indicated in darker shade than higher resilient states. Strategies through the wide passage are more resilient.

- **Reach-while-avoid control with multiple targets**: Here targets are entirely chosen based on the reaching path resilience.



- Tool link: https://bitbucket.org/stanlyjs/rescot/
- Paper link: https://people.mpi-sws.org/ kmallik/uploads/ResilientABCD2020.pdf