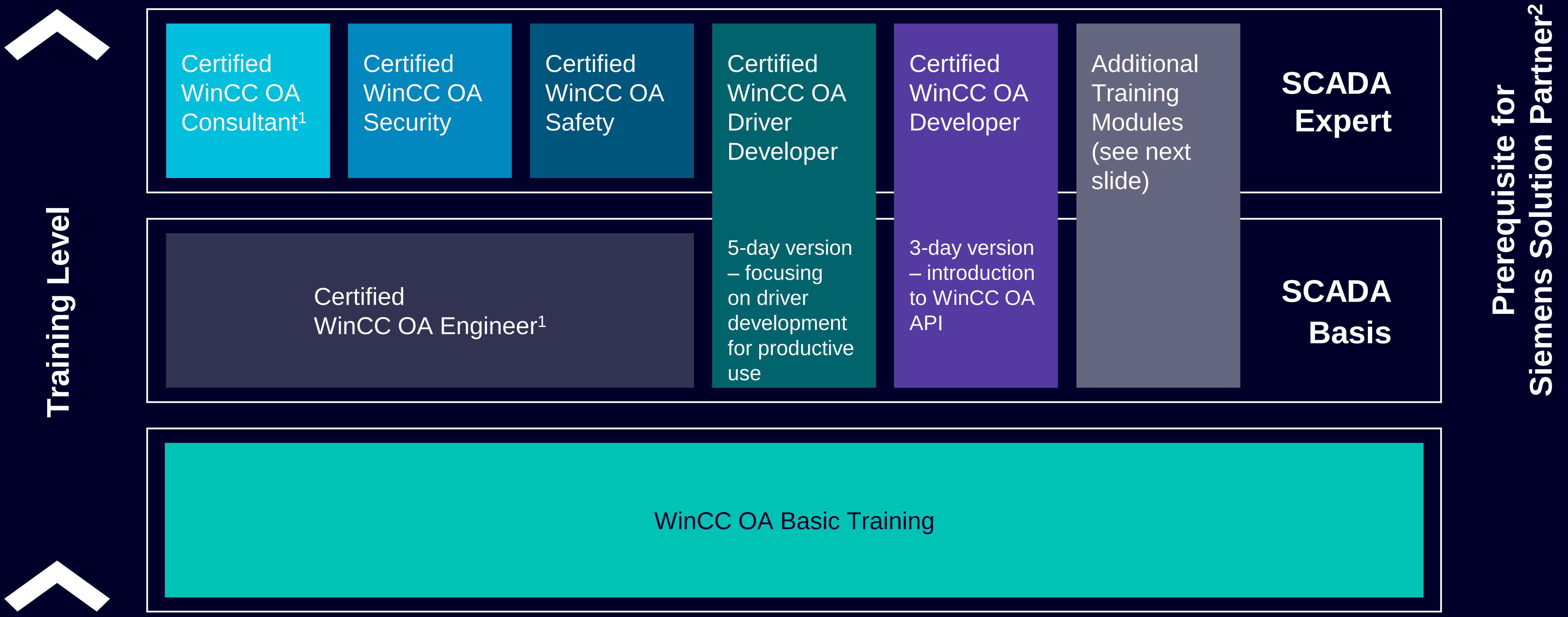
SIMATIC WinCC Open Architecture

Learning & Certification Path

SIEMENS

SIMATIC WinCC Open Architecture
Learning Path



Training Level

Certified WinCC OA Consultant[1]

Certified WinCC OA Security

Certified WinCC OA Safety

Certified WinCC OA Driver Developer

5-day version – focusing on driver development for productive use

Certified WinCC OA Developer

3-day version – introduction to WinCC OA API

Additional Training Modules (see next slide)

SCADA Expert

Certified WinCC OA Engineer[1]

SCADA Basis

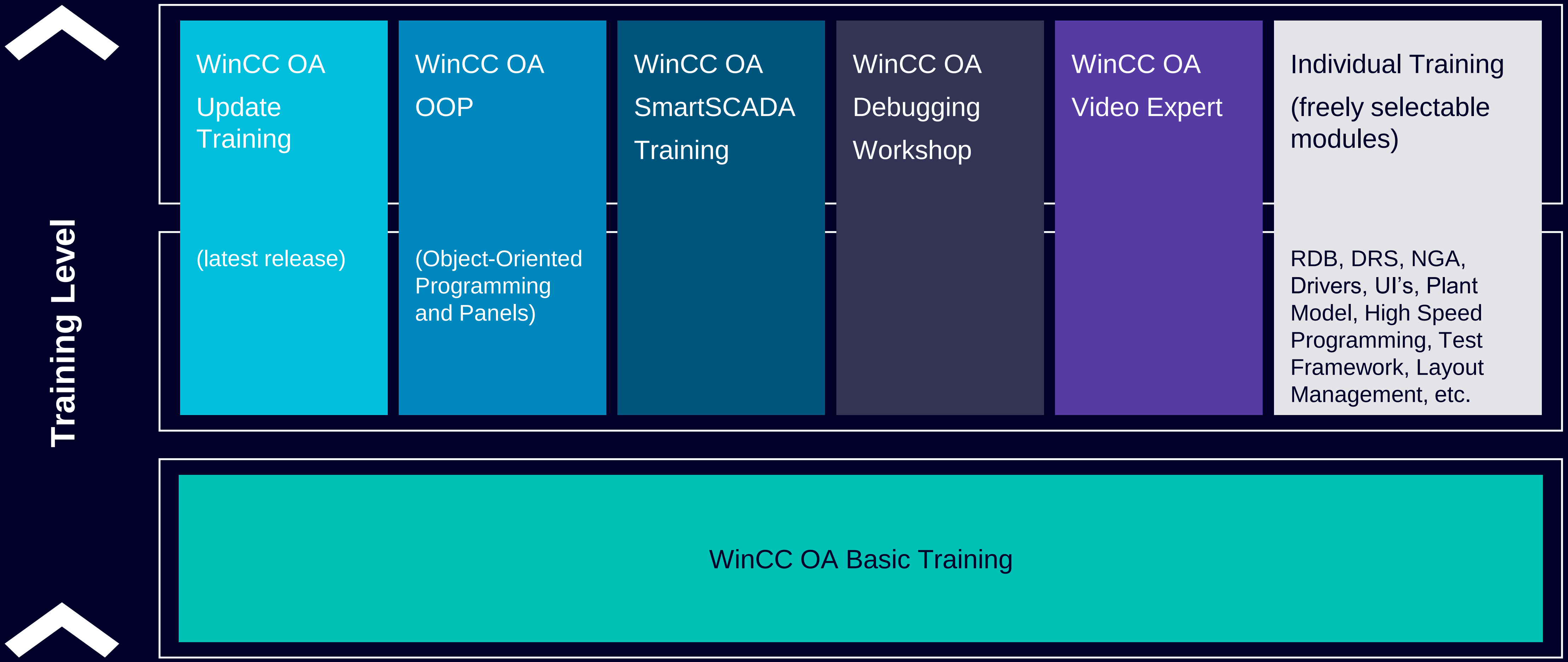
WinCC OA Basic Training

Prerequisite for Siemens Solution Partner[2]

[1] Between the WinCC OA Basic training, Certified WinCC OA Engineer WS and Certified WinCC OA Consultant WS we recommend 3 months of WinCC OA project-specific experience

[2] more details on following pages

SIMATIC WinCC Open Architecture
Additional Training Modules



Training Level

WinCC OA Update Training (latest release)

WinCC OA OOP (Object-Oriented Programming and Panels)

WinCC OA SmartSCADA Training

WinCC OA Debugging Workshop

WinCC OA Video Expert

Individual Training (freely selectable modules)

RDB, DRS, NGA, Drivers, UI's, Plant Model, High Speed Programming, Test Framework, Layout Management, etc.

WinCC OA Basic Training

SIMATIC WinCC Open Architecture
Community Program

SCADA Basis

2 certified WinCC OA Engineers

- Successful eTest at CEW (recertification every 2 years)
- Yearly update trainings (free of charge)

Solution Partner
Automation Drives
SIEMENS

SCADA Expert

SCADA Basis certification
+1 certified WinCC OA Consultant
& 1 certified WinCC OA Developer

- Successful eTest for recertification every 2 years
- Yearly update trainings (free of charge)

Solution Partner
Automation Drives
SIEMENS

WinCC OA OEM

2 certified WinCC OA Engineers &
2 certified WinCC OA Developers

- Standardized system/solution brand labeled as partner’s own solution/application required
- Yearly update trainings (free of charge)

SIMATIC WinCC OA
OEM PARTNER
etm

Besides the training qualifications in WinCC OA other prerequisites may apply according to Siemens Solution Partner Program and ETM OEM Partner Program

Disclaimer

©Siemens 2023

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g., use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cert.