

désignation type de produit	SOFTNET-PB DP-Slave V19 SOFTNET-PB esclave DP V19 ; logiciel pour esclave DP avec serveur OPC et logiciel de configuration ; Floating License logiciel Runtime, logiciel et manuel électr. sur DVD ; License Key sur clé USB ; classe A ; en 3 langues (de, en, cn) ; pour Windows® 10 Pro/Ent. ver. 21H2 ; 22H2; Windows® 11 Pro/Ent. ver. 21H2 ; 22H2; Windows® Server 2019, 2022 (Standard Edition, Datacenter) ; Windows® 10(IoT) Ent. 2019 LTSC Windows® 10(IoT) Ent. 2021 LTSC
	
Figure à titre d'exemple	
page de présentation technique du produit	https://l.siemens.com/1P6GK1704-5SW23-0AA0
version logicielle	V19
normes, spécifications, homologations	
fonction produit / pris en charge / Identification Link	Oui; selon IEC 61406-1:2022
Plus d'informations / liens Internet	
lien Internet	
• vers site Internet : Aide à la sélection TIA Selection Tool • vers site Internet : Communication industrielle • vers site Internet : SiePortal • vers site Internet : Banque d'images • vers site Internet : CAX-Download-Manager • vers site Internet : Assistance en ligne Industry	https://www.siemens.com/tstcloud https://www.siemens.com/simatic-net https://sieportal.siemens.com/ https://www.automation.siemens.com/bilddb https://www.siemens.com/cax https://support.industry.siemens.com
notes relatives à la sécurité	
notes relatives à la sécurité	Siemens commercialise des produits et solutions comprenant des fonctions de cybersécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux. Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire de mettre en œuvre - et de maintenir en permanence - un concept de cybersécurité industrielle global et de pointe. Les produits et solutions de Siemens constituent un des éléments de ce concept. Il incombe aux clients d'empêcher tout accès non autorisé à ses installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet dans la mesure où cela est nécessaire et seulement si des mesures de protection adéquates (ex : pare-feu et/ou segmentation du réseau) ont été prises. Pour plus d'informations à propos des mesures de protection pouvant être mises en œuvre dans le domaine de la cybersécurité industrielle, rendez-vous sur www.siemens.com/cybersecurity-industry. Les produits et solutions Siemens font l'objet de développements continus pour qu'ils soient encore plus sûrs. Siemens recommande vivement d'effectuer les mises à jour dès que celles-ci sont disponibles et d'utiliser la dernière version des produits. L'utilisation de versions qui ne sont plus prises en charge et la non-application des dernières mises à jour peut augmenter le risque de cybermenaces de nos clients. Pour être informé des mises à jour produit, abonnez-vous au flux RSS Siemens Industrial Cybersecurity à l'adresse suivante https://www.siemens.com/cert. (V4.7)
dernière modification :	21/01/2026 